

AIR FORCE  
INFORMATION DOMINANCE  
FLIGHT PLAN

THE WAY FORWARD FOR CYBERSPACE/IT  
IN THE UNITED STATES AIR FORCE



1 MAY 2015



## FOREWORD

Our nation relies on the internet and the systems and data of cyberspace for critical services. This reliance leaves us vulnerable to dangerous cyberattacks. The Secretary of Defense Carter recently provided the DoD cyber strategy for the department to work in concert with other federal agencies, the private sector, and international partners to “move quickly and efficiently to build the capabilities we need to defend the United States and its interests in the digital age.” When it comes to defending and warfighting in cyberspace, we must avoid group think by challenging thoughts, concepts, and bureaucratic inertia to best maintain and extend our operational advantages. We must be bimodal in providing rock-solid cyber capabilities for all missions while also acting with agility to capitalize on fast-evolving new opportunities.

The Air Force has already begun. The ability of our Airmen to imagine, integrate, and deliver superior, cyber-secure combat power has strengthened our Nation. Our strength stems in large measure from the ingenuity of our Cyber workforce, uniting with the rest of the operational community, industry, and academia, to deliver game-changing technological advancements and to maintain our operational advantages. Our collective efforts to ensure trusted and relevant information is available where and when needed will ensure that we are ready to fly, fight, and win the future fight... in air, space, and cyberspace.

This Information Dominance Flight Plan aligns with the strategies and objectives of the Air Force and the Department of Defense (DoD), to include the DoD Cyber Strategy and the Air Force’s Strategic Master Plan (SMP). This plan refocuses our Cyber workforce on executing, enhancing, and supporting Air Force core missions. This change in focus is critical as it strengthens our understanding of how cyberspace/Information Technology (IT) capabilities contribute to overall DoD operations and encourages the rapid development and integration of Air Force IT/cyberspace capabilities in support of joint warfighters and in the face of real and dangerous cyber threats to our core missions.

The Information Dominance Flight Plan projects forward 10 years. Cyberspace/IT functions are cardinal components of military operations; they foster freedom of action through the synergistic, multi-domain execution of capabilities. The Information Dominance Flight Plan provides the strategic framework that articulates the cyber challenges faced by the Air Force as well as vectors for moving forward across all core functions, mission areas, and Air Force components. It will help us to achieve this vision: The Air Force fully exploits the man-made domain of cyberspace to execute, enhance and support Air Force core missions. Your comments are welcome and can be directed to my Strategy and Policy Division - ([usaf.pentagon.saf-cio-a6.mbx.a6ss-workflow@mail.mil](mailto:usaf.pentagon.saf-cio-a6.mbx.a6ss-workflow@mail.mil)).

A handwritten signature in dark ink, reading "William J. Bender". The signature is fluid and cursive, with the first name being the most prominent.

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



## TABLE OF CONTENTS

Foreword .....	2
Executive Summary .....	5
Strategic Framework.....	9
Strategy .....	9
Measuring Success .....	10
Strategic Environment and Challenges.....	12
Directive Guidance – Information Dominance Vision .....	17
Strategic Goals .....	18
Goal 1: Provide Airmen trusted information.....	18
Goal 2: Organize, train, equip, and educate Cyber-Airmen to be experts in cyberspace .....	18
Goal 3: Deliver freedom of action in and through cyberspace .....	19
Goal 4: Optimize the PPB&E of cyberspace investments.....	19
Summary of Objectives and Initiatives .....	20
Objectives .....	24
Information Environment (IE) .....	24
Enterprise Services.....	25
Network Normalization.....	26
Future Air Force Bases .....	26
Policy .....	27
Enterprise Architecture.....	28
Cybersecurity.....	30
Task Force Cyber Secure .....	32
Spectrum .....	33
Force Development.....	34
Governance .....	35
Investment .....	36
Cyberspace Command and Control (C2) .....	38
Initiatives .....	39
Data Center Consolidation .....	39
Data Management.....	40
Single Security Architecture (SSA).....	41
Enterprise Operations Center (EOC).....	42
Aerial Layer Network (ALN).....	43
Base-Level Infrastructure.....	44
Combat Communications (Extending Services to the Tactical Edge) .....	46
Senior Leader Communications.....	48
Position, Navigation, and Timing (PNT).....	49
Cyberspace Capability Development and Innovation .....	50
Partnerships .....	51



Acquisition Reform.....	52
Summary .....	54





## EXECUTIVE SUMMARY

The United States Air Force's mission is to *fly, fight and win... in air, space and cyberspace*. This global mission requires exceptionally well-trained Airman and sophisticated systems. The Air Force protects and preserves our Nation's security interests, and offers freedom of action to our Joint and Coalition partners, by integrating capabilities to provide Global Vigilance, Global Reach, and Global Power.<sup>1</sup> This is the Air Force Vision,<sup>2</sup> achieved through unmatched execution of five core missions: air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control (C2).

This document provides a framework for coordinating movements by multiple organizations and thousands of individuals working to achieve **Information Dominance** for the United States Air Force. Information Dominance is the operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects. Airmen at every level need timely and accurate information to make decisions and act upon those decisions.<sup>3</sup> We often take information for granted and are surprised and frustrated when it is not available at the time of need and in the format required. All Airman performing missions need information to make the right decision - whether it's putting bombs on target, dropping humanitarian aid, uploading a software patch to satellite, designing base-level IT infrastructure, or even prescribing the right medical treatment. Every mission depends on information dominance, but our information advantages are increasingly at risk in and through cyberspace. Therefore, our vision is for the Air Force to fully exploit the man-made domain of cyberspace to execute, enhance and support Air Force core missions.<sup>4</sup>

Information Dominance enables warfighters at all levels of warfare to gain a deeper understanding of how adversaries operate and perceive their opponents. Information Dominance allows warfighters to gain detailed knowledge of the strategic, operational, and tactical environment, thus increasing the effectiveness of Air Force core missions across the multi-domain spectrum. Information Dominance provides tactical commanders with an awareness of available information, the information they actually need, and where to find and access it quickly in any situation. Achieving Information Dominance requires an ability to assess the veracity of the information we receive - this is a vitally important if we are to collect, gather, and deliver accurate and timely information decision-makers so that commanders have greater knowledge of the situation than the enemy.

The strategic aim is to push and pull viable and trusted information to and from Airmen as

<sup>1</sup> AF Global Vigilance, Global Reach, Global Power for America, 2013.

<sup>2</sup> US Air Force Vision, 2013.

<sup>3</sup> Command and Control (C2) is essentially about information: getting it, judging its value, processing it into useful form, acting on it, and sharing it with others. There are two basic uses for information. The first is to help create situational awareness (SA) as the basis for a decision. The second is to direct and coordinate actions in the execution of the decision. (Joint Pub 6-0).

<sup>4</sup> Air Force Core Missions: "air and space superiority; intelligence, surveillance, and reconnaissance; rapid global mobility; global strike; and command and control" 2014 America's Air Force: A Call To The Future.



effectively and efficiently as possible so they can make the informed decisions necessary to execute their mission. This aim demands changes to how we acquire systems, design tactics, and operate today. It moves us toward an integrated, multi-domain approach to operations. To meet this aim, we start by defining the three tenets for Information Dominance:

1. Increase effectiveness of Air Force core missions.
2. Increase cybersecurity of Air Force information and systems.
3. Realize efficiencies through innovative IT solutions.

Our Airmen need trusted information in place and across the spectrum of military capabilities to conduct their missions. There are many ways for users to communicate and interface among the networks and systems in the information environment; however, the more avenues users have to communicate and interface, the more risk there is for those systems to collect and deliver trusted information. Our systems need to be resilient and trustworthy, and the Cyber-Airmen who operate, maintain, and use the systems need expertise in exploiting and protecting key cyberspace terrain for the core missions to which they contribute. The four goals articulated in this document will move the Air Force toward improving mission assurance<sup>5</sup> and overcoming the challenges posed by systems-of-systems complexity and cyberspace vulnerabilities:

1. Provide Airmen trusted information where they need it so they can be most effective.
2. Organize, train and educate Cyber-Airmen to be experts in cyberspace and the Air Force core missions to which they contribute.
3. Deliver freedom of action in and through cyberspace to advance Air Force core missions
4. Optimize and prioritize the planning, programming, budgeting, and execution of cyberspace investments.

This Flight Plan articulates objectives that provide specific and measureable actions that will move the Air Force toward achieving each goal. The decision to focus efforts and resources toward these goals means we will focus on the highest priority items and cease efforts and investments on activities that are tangential or unrelated to our specified goals. The Core Function Support Plans (CFSPs) and Information Environment (IE) roadmaps will provide further detailed and actionable direction with respect to how the Air Force will meet its mission goals, to include how the Air Force will ensure IT/National Security System (NSS) investments in initiatives, programs, and systems align with DoD and Air Force priorities. The corporate

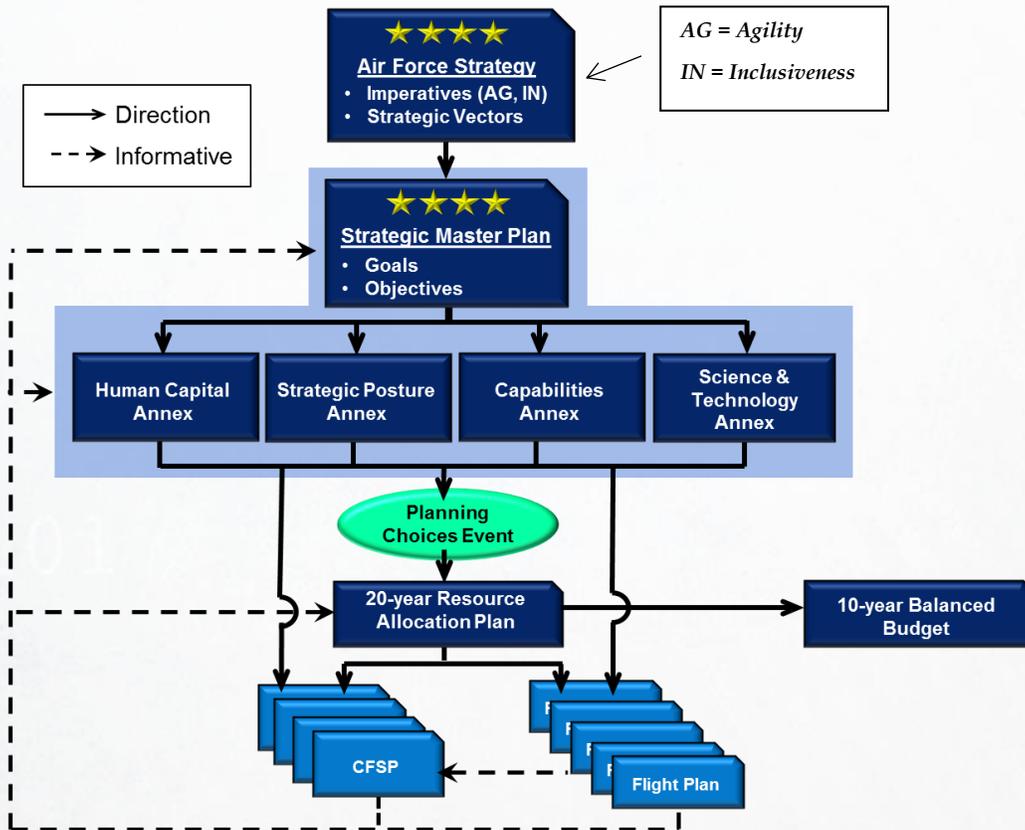
---

<sup>5</sup> Mission Assurance definition: “the process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains critical to the execution of DoD mission essential functions in any operating environment or condition” DoD Directive 3020.40.



portfolio management processes, in conjunction with the Air Force Strategic Master Plan, will appropriately align Air Force resources toward these ends.

The Information Dominance Flight Plan is a comprehensive document that aligns with the Air Force Strategic Master Plan. Figure 1 depicts the Air Force's strategic documents and associated plans and annexes.<sup>6</sup>



**Figure 1. AF Strategic Document Hierarchy**

The ability of the Air Force to meet DoD goals requires a fundamental change in cyberspace/IT management practices. Cyberspace/IT resources have historically been managed and acquired as stand-alone systems rather than as integral parts of a net-centric system-of-systems. As a result, duplicative investments of systems/platforms that deliver similar capabilities but are not interoperable are limiting the ability to effectively share information across the spectrum of military operations. Resourcing cyberspace/IT systems and platforms requires investment management not only at the Enterprise level (DoD Components), but also across the DoD

<sup>6</sup> United States Air Force Strategic Master Plan (February 2015).



defined Mission Areas.<sup>7</sup>

Mission Areas represent the major capability areas of the DoD to include interfaces to other National Security Activities. Mission Areas help ensure investments are accurately managed to meet compliance and statutory requirements. The Information Environment Mission Area (IEMA) represents the common, integrated information computing and communications environment of the Department of Defense Information Network (DoDIN) as well as how the Air Force executes, enhances, and supports joint warfighting priorities and creates a net-centric force capable of full spectrum dominance through information superiority<sup>8</sup>.

The purposeful integration of IT/cyberspace capabilities across these four mission areas ensures IT/NSS investments align with the Air Force's tenets of information dominance. Our ability to assure the five Air Force core missions (air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control (C2)) depends on our strength and capability in unifying efforts toward achieving the Information Dominance vision and the strategic goals described in this document.

---

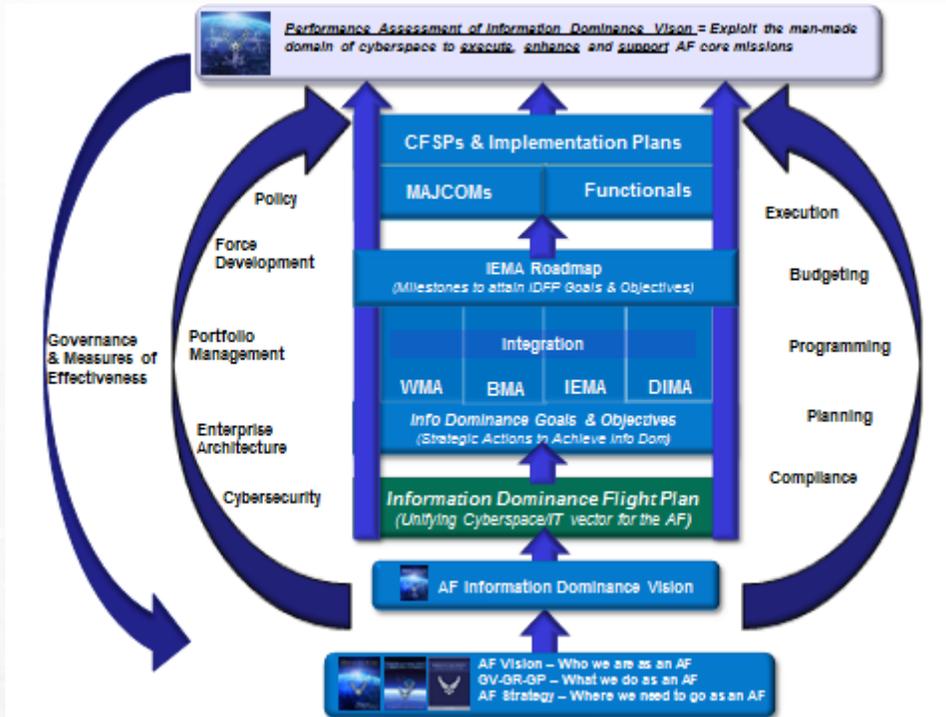
<sup>7</sup> Cyberspace/IT systems are synchronized and integrated across four Mission Areas to meet warfighter IT/NSS requirements: business mission area (BMA), information environment mission area (IEMA), defense portion of the intelligence mission area (DIMA), and warfighting mission area (WMA).

<sup>8</sup> Information Superiority: The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (JP 1-02).



## STRATEGIC FRAMEWORK

The Information Dominance strategic framework in Figure 2 illustrates the components and collaborative efforts involved in achieving and maintaining the operational advantages offered by information.



**Figure 2. AF Information Dominance Strategic Framework**

## Strategy

Strategy is set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national and/or multi-national objectives<sup>9</sup>. A successful strategy must coordinate the ends, ways, and means for achieving a desired course of action or the best approach to meet an end state.<sup>10</sup> Strategy has traditional applications across the military range of operations in peacetime and wartime environments. Any effective strategy is geared toward setting goals, designating actions to achieve those goals, and organizing mission

<sup>9</sup> Joint Publication 1-02.

<sup>10</sup> Liddel, B.H. (1991). *Strategy* (2d ed). New York: Penguin.



forces and resource to execute actions– strategy is about the desired and expected effects that actions will deliver. Strategy can be intentional or emerge as a pattern of activity as an organization adapts to its environment and involves both strategic planning and strategic thinking.<sup>11</sup>

Strategy can also be viewed as a way through a difficulty and an approach to overcoming an obstacle. Good strategy discovers critical challenges then designs a coordinated plan of focused actions toward resolution.<sup>12</sup> A good strategy has a basic underlying structure:

1. **Challenge:** A diagnosis or explanation of the nature of the challenge
2. **Vector:** A guiding policy or overall approach chosen to cope with or overcome obstacles identified in the diagnosis.
3. **Action:** Coherent steps that are coordinated with one another to support the accomplishment of the guiding policy.

This flight plan aims to unify the focus and efforts of the Air Force cyberspace/IT community by applying the basic principles of military strategy and the structure of good strategy.

### *Measuring Success*

Translating the Information Dominance Flight Plan vision and objectives into tangible actions (means) that will lead to the desired future end state requires a measurement framework.<sup>13</sup> This framework is essential in ensuring organizations across the cyberspace/IT community have a clear and actionable way ahead toward CIO goals and objectives. Although the objectives in the Information Dominance Flight Plan are measurable, they are written for use at the strategic level; to be actionable, they must be expressed as an integrated set of measures. This is achievable through a balanced scorecard approach, which enables organizations to implement long-term strategic goals through measurements of success and milestones. It is the framework for managing the implementation of strategy while allowing the strategy to evolve in responses to changes in the political and technological environment.<sup>14</sup>

Using the balanced scorecard criteria for performance measurement - customers, internal processes, financial aspects, and growth - we will be able to set and track metrics against the objectives outlined in the flight plan (Figure 3). This approach will provide a more balanced view of organizational performance and transform the Information Dominance Flight Plan from a broader strategic document into actionable activities. The balanced scorecard provides the

<sup>11</sup> Mintzbert, H. & Quinn, J.B. (1996). *The Strategy Process: Concepts, Context, and Cases*. New York: Prentice Hall.

<sup>12</sup> Rumelt, Richard (2011). *Good Strategy Bad Strategy: The Difference and Why It Matters*. New York: Crown Publishing Group

<sup>13</sup> Executive Guide: Effectively Implementing the Government Performance and Results Act (June, 1996, GAO/IGD-96-118).

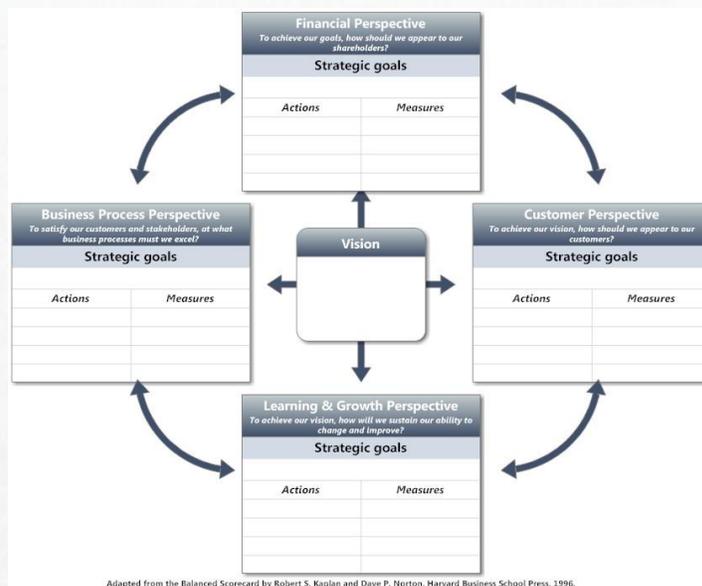
<sup>14</sup> Kaplan, R.S. & Norton, D.P. (January-February 1996). Using the Balanced Scorecard as a Strategic Management System. *Harvard Business Review*, 74(1), 75-85.



framework to:

- Communicate strategic goals across organizations
- Align and link strategic objectives to long-term goals
- Identify and align associated strategic initiatives
- Conduct periodic reviews to clarify and update the Information Dominance Flight Plan as needed

Through the balanced scorecard framework, the Air Force will identify what needs to be done and measured to execute the Information Dominance Flight Plan and improve strategic performance and results.<sup>15</sup> The framework will provide measurements of success to show how the Air Force will reach its end state for the flight plan objectives in terms of resources, time, and capability and also highlight any gaps or limiting factors in reaching the end state. Through the identification of actions, milestones, process owners, and resource, customer and capacity requirements, the balanced scorecard approach will support SAF/CIO A6 in 1) maintaining a consensus regarding requirements needed to achieve information dominance and the resources needed to satisfy those requirements; 2) providing a mechanism to help forecast developments; and 3) providing the framework and artifacts to help coordinate progress and identify/manage associated risks.



**Figure 3. Balanced Scorecard Framework<sup>16</sup>**

<sup>15</sup> Kaplan, R.S. & Norton, D.P. (January-February 1996). Using the Balanced Scorecard as a Strategic Management System, *Harvard Business Review*, 74 (1), 75-85.

<sup>16</sup> Adapted from Robert S. Kaplan and David P. Norton, "Using the Balanced Scorecard as a Strategic Management System, *Harvard Business Review*, 74 (1), 75-85.



## STRATEGIC ENVIRONMENT AND CHALLENGES

The United States Air Force's mission is to *fly, fight and win... in air, space and cyberspace*. This global mission requires exceptionally well-trained Airman and sophisticated systems. The Air Force protects and preserves our Nation's security interests, and offers freedom of action to our Joint and Coalition partners, by integrating missions to provide Global Vigilance, Global Reach, and Global Power.<sup>17</sup> This is the Air Force Vision,<sup>18</sup> achieved through unmatched execution of five core missions: air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control (C2).

Joint operations rely in part on cyberspace, the global operational domain within the information environment.<sup>19</sup> Cyberspace is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space.<sup>20</sup> Our ability to operate in and through the cyberspace domain benefits every core mission through improved speed, ubiquity, access, stealth, surprise, real-time battlespace awareness and information exchange, and effective command and control. Virtually every mission across the range of military operations depends on resilience and continued availability of a secure and trusted cyberspace domain. Every capability, mission, and member of the Air Force depends on information for success. Although the majority of the cyberspace domain is not under military or even U.S. Government control, the DoD operates within this global domain and defends our military operations, systems and information.

Cyberspace is distinct from other domains in that it is manmade without the apparent physical elements inherent in the air, land, sea, and space domains that provide recognizable, viable terrain for our adversaries<sup>21</sup>. Although not typical of the traditional "Clausewitzian" key terrain concepts, the cyberspace domain becomes recognizable through various physical elements such as fiber optic cables, databases, data centers, communication media, satellites, supply chains, and even the operators themselves<sup>22</sup>. These physical elements help in our ability to understand and assess the mission-relevant Cyber Key Terrain (CKT) and its associated vulnerabilities and threats. CKT is defined as any locality or area within cyberspace, the seizure or retention of which affords a marked advantage to either combatant (JP 1-02). CKT changes with the mission and adversary and may exist in many forms (to include links, RF communications, and spectrum) thus requiring a keen awareness and understanding how an adversary operates and how to anticipate their next move. As a result, recognition and understanding of both Joint and coalition CKT is critical in increasing Mission Assurance, enhancing resiliency of systems, and mitigating risk/vulnerabilities of our cyberspace/IT

<sup>17</sup> AF Global Vigilance, Global Reach, Global Power for America, 2013.

<sup>18</sup> US Air Force Vision, 2013.

<sup>19</sup> Joint Publication 3-13 (5 Feb 2013).

<sup>20</sup> Ibid.

<sup>21</sup> Mills, John R. (2013). Key Terrain of Cyber. *Georgetown Journal of International Affairs*.

<sup>22</sup> Ibid.



systems and platforms.

Although risks exist in every domain, the globally interconnected nature of cyberspace and the operational need for Air Force systems to “trust” each other create an immense exposure to operational risk. A cyberspace vulnerability in any one system introduces potential risk to all systems and, by extension, the missions and information on those systems. This domino effect not only puts DoD systems at risk, but also puts at risk those commercial systems on which the DoD depends for mission operations. This is the “physics” of cyberspace. However, unlike risks inherent in the physics of other operational domains, we can effectively mitigate vulnerabilities and manage risk in cyberspace through the manipulation of the domain itself.

Threats to United States’ cyberspace operations are increasing through ease of access to capabilities once only held by the most advanced and progressive nations. Advances in adversarial capabilities in space control and cyberspace warfare challenge U.S. freedom of action. Some of these capabilities are attained with relatively minimal cost, greatly reducing the barriers to entry that have historically limited the reach and power of non-state actors, organized militias, and radical extremists.

We live in an age when individual acts can yield powerful and global strategic effects. Today’s strategic environment presents a broad range of threats, ranging from non-state actors to more advanced nuclear nations. This global environment requires United States forces to have flexibility, versatility, and the ability to shift to inherently agile, deployable, networked, and sometimes multi-function systems from those designed for fixed purposes or limited missions.<sup>23</sup>

Accurate predictions within the cyberspace/IT environment present significant challenges. Rapid advances exploited by growing and increasingly sophisticated international competitors have created an environment today in which operational and strategic risks introduced by cyberspace vulnerabilities are both diffuse and potentially catastrophic. Our contemporary cyberspace forces are faced with a proliferating array of mission systems with ever more mutual dependencies which present unexpected cyberspace vulnerabilities. These system proliferation challenges reflects the Air Force’s past approach of purchasing systems tailored for individual purposes rather than integrating warfighting capabilities through collaborative and interdisciplinary cyberspace/IT systems.

The growing awareness of the operational need for standardization with the DoD Information Networks and the need to respond to adverse cyberspace intrusions drives the requirement to migrate to an integrated operational domain. Air Force systems now require a secure, robust architecture that is cost-effective and able to adapt to and incorporate emerging technologies while mitigating vulnerabilities. Doing so provides joint warfighters with the right capabilities and systems to both defend the networks supporting operations as well as conduct operations

---

<sup>23</sup> USAF Posture Statement, 2014.



against adversaries. The Air Force will pursue every opportunity to ensure architectures, systems, and network processes are standardized and integrated as much as possible within the joint operating environment.

Defense of the Air Force Information Network is conducted through Air Force cyberspace operations, specifically by Cyber-Airmen conducting Department of Defense Information Network Operations (DoDIN Ops) and Defensive Cyberspace Operations (DCO) in coordination with other services and agencies of the government. However, the relative advantage in expertise enjoyed by the United States (and the Air Force's ability to recruit talent) is under pressure as a greater percentage of college degrees in science, technology, engineering, and mathematics (STEM) are increasingly awarded to citizens of competitor-nations, even to include those from American universities.<sup>24</sup>

Air Force networks and systems are under constant attack and therefore must be resilient and protected to mitigate adversarial actions as well as disruptions caused by natural means and technological mishaps. Mission Assurance provides the framework in which the Air Force will prioritize cyberspace/IT investments to retain the ability to ensure the efficiency and effectiveness of operations, ensure the optimal and secure performance in a fiscally-constrained environment, and ensure the resiliency of systems during mission operations. Although Mission Assurance<sup>25</sup> is often viewed as a strategy, it provides the common frame for the Air Force to vet and prioritize protection and resiliency efforts and reduce risk across the spectrum of mission systems and platforms. Mission Assurance is critical to fulfilling the Information Dominance vision and addressing the complexity of cyberspace/IT vulnerabilities within the joint operating environment.

The increasing commercial and DoD demand for spectrum, technological innovation, and the rising proliferation of adversary anti-access technologies drive the need for the DoD to modify and innovate the methods in which it uses spectrum.<sup>26</sup> With few federal regulatory requirements and incentives to use spectrum more efficiently, and the reliance on individual agencies to ensure the systems they develop are as spectrum efficient as possible, we do not have the full freedom of access needed to operate in an advanced technological environment.<sup>27</sup> To provide the spectrum efficiency needed to meet mission needs, the Air Force must become more efficient, flexible, adaptable, innovative, and agile in its use of spectrum to not only have access when required, but also for the successful execution of Air Force core missions.

Emerging global trends provide further insight and establish context to inform cyberspace

<sup>24</sup> Department of Commerce 2012 report on competitiveness,

[http://www.commerce.gov/sites/default/files/documents/2012/january/competes\\_010511\\_0.pdf](http://www.commerce.gov/sites/default/files/documents/2012/january/competes_010511_0.pdf).

<sup>25</sup> Mission Assurance definition: "the process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure and supply chains critical to the execution of DoD mission essential functions in any operating environment or condition" DoD Directive 3020.40.

<sup>26</sup> 2013 Electromagnetic Spectrum Strategy

<sup>27</sup> GAO Report on Spectrum Management (2004)



directions. Some of these emerging trends in technology indicate a closer human-machine interface that includes cloud computing, smart machines, continued proliferation of mobile devices, the “Internet of Things,” and software-defined everything.<sup>28</sup> Combat capability improves with agility: the ability to adapt to a changing environment to gain and maintain information dominance despite emerging, highly adaptable and asymmetric adversaries and threats (whether they are nation states or non-state actors).

Some of the specific challenges SAF/CIO A6 foresees for the Air Force in building, extending, and securing the Air Force cyberspace domain toward 2025 include the following:<sup>29</sup>

1. Solving communications and computing constraints related to Tactical Edge environments (disconnected or intermittent connectivity, limited throughput, high latency and jitter, and low-power)
2. Ensuring the electromagnetic spectrum is available for future military usage in the face of mounting commercial pressures at home and abroad, complicated regulatory and contested/congested electromagnetic environments during training and conflict
3. Leveraging the explosion in end-user mobile devices and capabilities in balance with cybersecurity
4. Addressing Information Security pertaining to data aggregation as the DoD moves to a broader use of a cloud construct
5. Converging redundant base-level infrastructures to support different service components, joint tenants, and the Intelligence Community (IC)
6. Supporting research toward software-defined networks as contributors to Air Force core missions
7. Competing successfully to recruit, educate and retain excellent Cyber-Airmen for government service in a highly-dynamic and competitive sector of the U.S. economy
8. Effectively leveraging existing organizations for cyberspace innovation to include industry and private partners
9. Remaining committed to integration throughout the lifecycle of weapon system development in the face of fiscal reductions

For mission success in tomorrow’s congested and contested information environment, the Air Force requires centralized strategic direction in developing and sustaining operations in and through cyberspace. To address the challenges described above, the Air Force needs unity of

<sup>28</sup> See “Air Force Cyber Vision 2025” by AF/ST.

<sup>29</sup> Note: USAF systems used for C2 shall comply with standardization requirements but will remain independent from IT networks.



effort and optimized investments to better afford seamless interoperability, resilience,<sup>30</sup> and flexibility that will be both responsive to technological change and affordable in the resource-constrained environment.

---

<sup>30</sup> Network Resilience: A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. (CNSS Instruction 4009).



## DIRECTIVE GUIDANCE - INFORMATION DOMINANCE VISION

The Air Force fully exploits the man-made domain of cyberspace to execute, enhance and support Air Force core missions.<sup>31</sup> This vision provides an aim point for coordinated action by many organizations in the Air Force working together to maintain information dominance.<sup>32</sup> Three prioritized tenets help guide efforts toward achieving the vision:

1. **Increase effectiveness of Air Force core missions:** How operations in cyberspace enable the successful execution of Air Force core missions by ensuring information is both timely and accurate.
2. **Increase cybersecurity of Air Force information and systems:** How activities in cyberspace foster the security of Air Force information and minimizes the vulnerabilities of host systems as well as the systems of systems to which they connect by applying a holistic approach to cybersecurity that encompasses people, culture, and operational processes.
3. **Realize efficiencies through innovative IT solutions:** How to leverage technology and resources in a manner that ensures minimal to no capability gaps or overlaps, shortens our kill chains, rapidly develops and acquires relevant capabilities, and makes better, faster decisions while understanding and managing the associated risks. This is accomplished by identifying, vetting, funding, and implementing innovative ideas from Airmen to realize our full potential and meet future needs.

Applying these tenets requires informed judgment by Cyber-Airmen<sup>33</sup> and the support of the Science and Technology, Engineering, and Acquisition communities. The tenets help focus and steer Air Force actions and decision-making about information and provide the framework to make informed investment decisions. Striving to achieve this vision propels us to fully exploit cyberspace.

The Information Dominance Flight Plan aligns to the *America's Air Force: A Call to the Future* (Air Force Strategy) and the DoD CIO strategy for information resource management. This Information Dominance Flight Plan is also aligned with the Air Force's Strategic Master Plan (SMP), the authoritative guidance for the CFSPs. The Air Force SMP ensures long-range Air Force strategy, policy, and guidance are accurately incorporated to inform planning and programming decisions. The Information Dominance Flight Plan is structured to inform the SMP annexes and CFSPs, which translate SMP goals, objectives, and initiatives into tangible cyberspace/IT actions and priorities.

<sup>31</sup> Air Force Information Dominance Vision, 2015.

<sup>32</sup> Information Dominance: The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects." (Air Force Information Dominance Vision).

<sup>33</sup> Cyber-Airmen are specifically trained by the Air Force to directly execute, enhance, and support Air Force core missions in and through cyberspace with a common, air-minded set of cyber-skills. (Air Force Information Dominance Vision).



## STRATEGIC GOALS

To realize the Air Force Information Dominance Vision, the Air Force will execute a set of coherent actions that focus limited resources on achieving the following four strategic goals.<sup>34</sup>

*Goal 1: Provide Airmen trusted information where they need it so they can be most effective.*

Airmen at all levels in the Air Force use timely and accurate information to make informed decisions. The Air Force will achieve greater collaborative efficiency across the DoD and with external mission partners by bringing Air Force IT architectures, systems and processes into compliance with the Joint Information Environment. We will compress the information flow within the kill chain and apply common data standards in all mission areas. We will leverage opportunities to manage information and develop a data management plan to ensure data veracity as well as the accessibility of information to mission users and analysts. Air Force core missions benefit from all of these actions through greater operational and technical resilience, improved interoperability and effectiveness, enhanced integration across information systems, faster capability delivery, prioritized secure capabilities, and reduced costs.

*Goal 2: Organize, train, equip, and educate Cyber-Airmen to be experts in cyberspace and the Air Force core missions to which they contribute.*

The Air Force will continue its long-standing tradition of fostering and promoting innovation, especially in leveraging cyberspace. We will improve our policies and training/education programs to foster a workforce of highly skilled and qualified Cyber-Airmen who execute, enhance and support Air Force core missions. Cyber-Airmen will be experts not only in cyberspace, but in the core missions to which they contribute. Cyber-Airmen will also receive specialized training to ensure they are proficient within the system/platform to which they are assigned. This includes continuous training and education throughout their careers to allow for the development of the advanced skill sets needed to operate and defend cyberspace mission systems. We will also focus on the education and training of our civilian personnel to better leverage their skills and foster collaborative workplace environments. Additionally, the Air Force will recruit STEM professionals to lead and operate within the cyberspace career field as well as educating and training personnel outside of the cyberspace community to gain the best understanding of how cyberspace contributes to the overall Air Force mission.

<sup>34</sup> Goal: An expression of the desired future state of the Air Force in a particular area or theme. Goals define and prioritize broad direction, and are inherently long-term in nature. (Air Force Strategic Master Plan).



*Goal 3: Deliver freedom of action in and through cyberspace to advance Air Force core missions.*

Freedom of action in cyberspace through the application of mission assurance<sup>35</sup> is a prerequisite for successful Air Force core mission execution. Having freedom of action mitigates bad actors' attempts to interfere with operations. It also allows the Air Force to deliver more combat power by exploiting cyberspace's unique characteristics. The Air Force will integrate cybersecurity throughout the lifecycle of weapon system development in all mission areas and will focus efforts on keeping information secure. As a man-made domain, cyberspace is fertile ground for game-changing innovation; innovative ideas of our Airmen will be rapidly identified, vetted, funded, and implemented across the Air Force to maximize potential and meet future Air Force needs.

*Goal 4: Optimize the planning, programming, budgeting and execution of cyberspace investments.*

Investments and spending on cyberspace capabilities across the core functions will be fully transparent and aligned with this flight plan and subsequent roadmaps. The Air Force will use a flexible and dynamic process of Capital Planning and Investment Control (CPIC)<sup>36</sup> for cyberspace technology to ensure its competitive advantages are realized and to maximize investments expected to enhance Air Force core missions. A competitive advantage is realized by the Air Force's ability to outperform adversaries in terms of capabilities and the development/implementation of more advanced systems. Improved alignment of spending will provide additional resources for modernization and further innovation. The Air Force will ensure that IT/cyberspace compliance requirements are uniformly applied throughout the Air Force enterprise. SAF/CIO A6 will assist programs (through collaboration and cooperation with SAF/AQ) that acquire cyberspace/IT capabilities early in the acquisition processes. This will improve agility, responsiveness, unity of efforts, and the Air Force's ability to implement best practices in cyberspace/IT investments.

<sup>35</sup> Mission Assurance definition: process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the execution of DoD mission-essential functions in any operating environment or condition. (DODD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*).

<sup>36</sup> CPIC is an IT portfolio-driven management process for ongoing identification, selection, control and evaluation of investments. This process attempts to link budget activities and agency strategic priorities with achieving specific IT program modernization outcomes. (DOD/DCMO "Guidance for Defense Business Systems Funds Certification and Defense Business System Integrated Program/Budget Review"). The IT portfolio includes all programs registered in the Enterprise Information Technology Data Repository (EITDR).



## SUMMARY OF OBJECTIVES AND INITIATIVES

The Information Dominance Flight Plan is supported by specific, measurable, achievable, realistic and time-bound (SMART) strategic objectives<sup>37</sup> designed to meet the goals and overcome the challenges foreseen over the next decade. Supporting the objectives are strategic initiatives which comprise specific projects or tasks necessary toward the goals and objectives. The tables below highlight the strategic objectives and supporting initiatives essential to ensuring the Air Force will reach our strategic goals:

<b>Goal 1: Provide Airmen trusted information where the need it so they can be most effective</b>	
<b>Strategic Objectives</b>	<b>SMP Linkage<sup>38</sup> (reference item)</b>
1.1: Increase opportunities to bring Air Force information environment architectures, systems, and processes in compliance with JIE by 4Q FY19	FH2.4.C5
1.2: Develop and use the AF Enterprise Architecture to guide investment strategies and establish the Architecture Executive Committee to govern initiatives and update AF policy to guide the development of and use of architecture NLT 4Q FY16	AG2.1
1.3: Divest of those organic services DoD(e.g., DISA) provides as an Enterprise Service that meet AF requirements NLT 2 FYs after the service is available at a sufficient scale from DISA – divestment of services will be based on an IT service commodity business case analysis to show SAF/CIO the cost-benefit of divesting	FH2.4.C5
1.4: Increase IT system efficiency by standardizing Unified Capabilities for Air Force Connectivity to the DoDIN by 4Q FY17	FH2.4.C5
1.5: Modernize AF Spectrum Management process IAW Joint Electromagnetic Spectrum Operations CONOPS, including adopting the DoD Spectrum Management System by FY17	FH2.4.C4
<b>Supporting Strategic Initiatives</b>	<b>SMP Linkage</b>
1.1.1: Deploy an Authorization Infrastructure to dynamically control authorized user access to information by 4Q FY19	FH2.4.C5
1.1.2: Transition all Air Force data-centers to JIE construct (e.g., IPN/cloud) by 4Q FY17 (APCs/RDCs to be divested by 4Q FY18)	FH2.4.C5
1.1.3: Move to a resilient JIE SSA <sup>39</sup> by replacing all AF gateways with a JRSS <sup>40</sup> by 4Q FY17	FH2.4.C5
1.1.4: Develop a roadmap for implementing DoDI 8320.02 data standards by 4Q FY15	AG2.1

<sup>37</sup> Objective: A major milestone or action required to achieve a goal. It produces a tangible result. (Air Force Strategic Master Plan).

<sup>38</sup> Nomenclature aligned to Air Force Strategic Master Plan Vectors (SMP): AG=Agile; FH=Full-Spectrum-Capable, High-End-Focused; IN=Inclusiveness; MDA=Multi-Domain Approach to our Five Core Missions.

<sup>39</sup> Single Security Architecture.

<sup>40</sup> Joint Regional Security Stack.



<b>Goal 1 (continued)</b>	
<b>Supporting Strategic Initiatives</b>	<b>SMP Linkage</b>
1.1.5: Upgrade SLC3S <sup>41</sup> communications systems to fleet to IP infrastructure as a primary means by 4Q FY19; use link diversity to assure unbroken, survivable communications on specific SLC3S elements	FH2.4.C6
1.1.6: Implement a plan to reduce costs by a goal of 10% annually through the rationalization all Air Force applications through the PfM/CPIC process with a focus of providing Airmen less and better systems to accomplish the mission NLT FY18	FH2.4.C5
1.1.7: Develop a roadmap to enable information sharing or interoperability and collaborative agreements (to include multi-level security capability for cross-domain information sharing) with industry and coalition partners for implementation by FY20	FH2.4.C2 IN2.3.P1
1.1.8: Evaluate the RAND Combat Communications Demand Study NLT end of FY15 and modify Combat Communications force structure as required	FH2.2
1.1.9: Evolve Air Force Network Operations Squadrons to be complaint with JIE EOC <sup>42</sup> standards by 4Q FY19	FH2.4.C5
1.1.10: Develop a plan to optimize, align, and support Air Force CIO equities in PNT Enterprise Management and Integration by 4Q FY16	FH1.4.C4
1.4.1: Develop recommendations for providing modern platforms including mobile solutions to enable airmen with the right tools to perform their mission by 4Q FY17	FH2.4

<b>Goal 2: Organize, train, equip, and educate Cyber-Airmen to be experts in cyberspace and the Air Force core missions to which they contribute</b>	
<b>Strategic Objectives</b>	<b>SMP Linkage</b>
2.1: Improve the workforce by developing a cyber aptitude assessment for augmentation of/inclusion in accession by 4Q FY17	AG1.2.H1
2.2: Implement programs to attract and retain recruits with prior cyber-skills, experience and certification with incentive programs by 4Q FY18	AG1.1.H1.4
2.3: Ensure every Cyber-Airmen position in the Air Force has Initial Qualification Training (IQT) associated with it by 4Q FY 19	AG1.2.H1
2.4: Improve mission assurance at the wing-level in each MAJCOM by developing and implementing Cyber Squadron of the Future PAD by 4Q FY18	AG3.3.H1
2.5: Develop and implement a plan for civilians in appropriate cyberspace positions to receive military-equivalent cyberspace training (e.g., Cyber 200/Cyber 300) by 4Q FY18	AG1.2.H1.2

<sup>41</sup> Senior Leader Command Control Communications System (a.k.a. VIP Special Air Mission fleet).

<sup>42</sup> Enterprise Operations Center



<b>Goal 2 (continued)</b>	
<b>Supporting Strategic Initiatives</b>	<b>SMP Linkage</b>
2.2.1: Develop and implement a plan to certify IT acquisition personnel as Program Managers by 4Q FY19	AG1.2.H1.2
2.3.1: Shorten 333 Training Squadron Course Resource Estimate timeline for implementation of training course changes to 120 days from determination of a need NLT 4Q FY17	AG1.2.H5

<b>Goal 3: Deliver freedom of action in and through cyberspace to advance Air Force core missions</b>	
<b>Strategic Objectives</b>	<b>SMP Linkage</b>
3.1: Develop recommendations to amend the cybersecurity Assessment & Authorization process to include a risk management framework process NLT 4Q FY16	FH1.3
3.2: Develop an all-inclusive operational cyberspace JIE-aligned C2 construct NLT 2Q FY16	FH1.3
3.3: Improve dissemination and develop penetration metrics for DAMO <sup>43</sup> and DIB <sup>44</sup> reports and analytics to facilitate corrective actions for Air Force missions by 1Q FY15	FH1.3
3.4: Establish and lead a Cyberspace Security and Operations Task Force to develop recommendations and a roadmap to enhance and enable the warfighters' ability to execute Air Force core missions in and through cyberspace by 4Q FY16.	FH1.3
3.5: Test new cryptographic technologies within one year of market availability for applicability and modernization of Air Force use	FH1.3
<b>Supporting Strategic Initiatives</b>	<b>SMP Linkage</b>
3.2.1: Work with DISA to develop and deliver a joint C2/Service desk construct to enable EOC operations NLT 4Q FY17	FH2.4.C5
3.2.2: Designate a Cyberspace Innovation Center to identify, vet, fund, and implement information and cyberspace innovations to increase the Air Force's competitive advantages in its core missions. IOC by 4Q FY16	GCT.1 AG1.2.H1 AG3.3.H1

<sup>43</sup> Damage Assessment Management Office.

<sup>44</sup> Defense Industrial Base.



<b>Goal 4: Optimize the planning, programming, budgeting, and execution of cyberspace investments</b>	
<b>Strategic Objectives</b>	<b>SMP Linkage</b>
4.1: Transform information and information systems policy by creating a 17-series of publications by 4Q FY16	AG3.3
4.2: Improve financial efficiency and warfighting effectiveness by developing and implementing a Capital Planning and Investment Control Process for implementation in WMA, BAM, DIMA, IEMA NLT 4Q FY16	AG3.3
4.3: Increase effectiveness of Enterprise Information Dominance Governance (EIDG) by establishing policy to describe the EIDG structure, roles, and responsibilities and their relationship to the IDFP	AG2.5.C2
4.4: Release a revised Information Dominance Flight Plan to inform the Air Force Corporate Process and the AF Strategic Master Plan NLT 3Q of each odd-numbered FY	AG3.3
<b>Supporting Strategic Initiatives</b>	<b>SMP Linkage</b>
4.2.1: Increase agility in responding to the cybersecurity and technological operational requirements (through collaboration and cooperation with SAF/AQ) by ensuring key systems are designed, engineered, tested, acquired, and sustained smartly and efficiently and streamline the IT acquisition process. NLT 1Q FY16	AG2.1
4.2.2: Implement a human capital investment strategy to maintain currency of cyber forces NLT 4Q FY16	AG1.1.H1.4
4.3.1: Through the corporate process, provide strategic direction and investment inputs for the Air Force CIO to ensure airborne networking investments improve warfighting effectiveness across mission areas	FH1.1.C3
4.3.2: Develop a plan to improve cybersecurity implementation & test capabilities as well as reduce procurement hurdles through effective development of policy NLT 1Q FY16	AG2.3
4.3.3: Plan for, identify, and provide POM inputs for AFISMC core services and manpower requirements NLT 2Q FY16	AG3.3



## Objectives

### Information Environment (IE)

The Air Force's information environment<sup>45</sup> evolved and converged as individual mission needs dictated, rather than being designed. The maturation of Joint employment concepts over the past twenty years of conflict has driven an awareness of the advantage of consolidation. Likewise, the need for increased security and situational awareness of the environment as a whole led the DoD to drive towards a Joint Information Environment (JIE)<sup>46</sup> that standardizes



across the DoD and collapses security boundaries. Warfighting, intelligence, and business or functional systems critical to operations are included in the JIE, as well as common services, such as email and other administrative and collaborative tools, storage and backup. Although JIE includes some intelligence systems, the bulk of these systems will be enhanced under the Intelligence Community Information Technology Enterprise (ICITE) initiative, which is very similar in intent to the DoD's JIE undertaking. JIE and ICITE are similar, the two being developed with closed coordination between DoD and the intelligence community.

**Challenge:** The DoD information environment is a complex layering of multiple networks with overlapping, duplicative roles and responsibilities<sup>47</sup>. Increased threats from both known and unknown adversaries on our cyberspace/IT systems drive the need for a more agile and defensible network that will meet the needs of our military operational environment while responding to the complexity of information systems. The DoD is now faced with building and sustaining a standardized and modern network architecture that will improve mission effectiveness, increase cyber security, reduce cost, and optimize cyberspace/IT efficiencies. Additionally, the need for the Air Force to share data and collaborate with coalition partners drives an increased focus on our Mission Partner Environment (MPE). The MPE is an operating environment in which the joint force and its coalition partners plan, prepare, and execute operations at a single security classification level with a common computing language; the MPE provides flexibility at strategic, operational, and tactical levels so that CCDRs can execute C2

<sup>45</sup> Information environment: the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). The Information Dominance Flight Plan addresses the cyberspace/IT systems, networks, and processes that reside within the information environment.

<sup>46</sup> The JIE is a secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies, JIE CONOPS, 25 Jan 2013.

<sup>47</sup> JIE Operations CONOPS, 25 Jan 2013.



and achieve the desired operational effects.<sup>48</sup> In the JIE construct, we must ensure that our systems can continue to host coalition systems such as CENTRIXS and Pegasus so that the MPE retains its ability to support mission requirements.

**Vector:** The end state will be a shared IT infrastructure for all of DoD common enterprise services and a single security architecture protecting DoD information networks while eliminating redundancies and improving resiliency across the components. It will facilitate the exchange of information and intelligence across all DoD components, within a secure, robust and standardized architecture that is better able—through incorporation of standards and practices—to adapt to and incorporate emerging technologies, such as mobile wireless devices and applications. The Air Force will leverage JIE to provide greater accessibility to necessary computing, applications for improved cyberspace operations across the core missions. JIE will also validate and prime viable data to develop consolidated standards that will shape technology and rapid capability development as well implement innovative IT capabilities.

**Action:** The Air Force will increase opportunities to bring Air Force information environment architectures, systems, and processes in compliance with JIE by 4Q FY17. This includes the development of recommendations for providing modern platforms including mobile solutions to enable airmen with the right tools to perform their mission.

---

## Enterprise Services

**Challenge:** Enterprise Services fall into four categories: Enterprise Applications (e.g., email), Identity and Access Management, Infrastructure, and Mobility. Enterprise Services change over time as new services become popular and legacy services become obsolete or vulnerable to attacks. The changing nature of Enterprise Application requires the Air Force to develop new methods in delivering enterprise services that are consistent across core mission systems.

**Vector:** The DoD CIO in coordination with each Service is providing and planning candidate Enterprise Services to support customer-facing capabilities, machine-to-machine services, and infrastructure services for the entire department. Providing a consistent set of enterprise services will help ensure that joint warfighters and their mission partners can discover, access, and use information assets to achieve mission success, no matter where the information resides, while also delivering Airmen increased capabilities at lower cost to support core missions.



**Action:** The Air Force will divest of those organic services DISA provides on an Enterprise

---

<sup>48</sup> JIE CONOPS, 18 Sep 2014.



Service that meet Air Force requirements, NLT 2 FYs after the service is available at a sufficient scale from DISA – divestment of services will be based on an IT service commodity business case analysis to show SAF/CIO the cost-benefit of divesting certain organic services.

---

### Network Normalization

**Challenge:** The consolidation of installation cyberspace/IT services demands the sharing of resources among multiple capabilities, devices and services. The lack of standardized networks prevents interoperability among cross-service missions and mission systems thus reducing mission effectiveness. The Air Force needs to consolidate those networks that employ common operational standards.

**Vector:** Network Normalization improves the resiliency of modern infrastructure to support mission operations and cyberspace-defense through common networks and TTPs. Under JIE, the shared IT infrastructure will look, feel, and operate the same regardless of service provider and usage (mission specific). JIE will provide standardized networks to increase mission effectiveness and improve cybersecurity, performance and the ability to connect to the DoDIN through government owned or leased connections by terrestrial, wireless, and satellite links.

**Action:** The Air Force will increase IT system efficiency by standardizing Unified Capabilities for Air Force connectivity to the DoDIN by 4Q FY17.

---

### Future Air Force Bases

**Challenge:** While the Air Force continues to integrate our execution capabilities across mission areas and components, we also defend the enterprise “commons” upon which those capabilities we depend to exchange information – the Air Force portion of the cyberspace domain. As the Air Force transitions toward JIE, the need to employ a defense-in-depth approach becomes increasingly important to support enterprise defense requirements.

**Vector:** The Air Force will continue to organize, train, and equip to provide for the defense of the Air Force’s cyberspace “commons” by Cyberspace Squadrons at our bases, including investment in appropriate tools and training for Cyber-Airmen, infrastructures that simplify situational awareness and C2, and initiatives that facilitate rapid acquisition of defensive capabilities in response to evolving threats. To improve situational awareness and cybersecurity of mission systems, the Air Force will enforce configuration standards to the device level<sup>49</sup> to facilitate automated reporting, centralized control, and effective vulnerability identification and remediation. The Air Force will also collapse public access points to create a smaller and better integrated “perimeter” that is patrolled by automated sensors and highly trained Cyber-Airmen and deploy TTPs to facilitate insider threat detection and prevention (for

---

<sup>49</sup> See 24 Air Force’s Base Area Network Functional Specification.



education and training missions, the use of a commercial or .edu network may be necessary to meet mission requirements). In cooperation with sister services and USCYBERCOM, the Air Force will develop skilled cyberspace mission forces with expertise in protecting information systems, and cyberspace and DoDIN mission systems.

**Action:** The Air Force will improve mission assurance at the wing-level in each MAJCOM by developing and implementing the Cyber Squadron of the Future PAD by 4Q FY18.

---

## Policy

**Challenge:** The Air Force has been slow in the development and delivery of timely cyberspace/IT policy and associated interim changes to meet the rapid pace of new systems and processes that support Air Force core missions. Effective policy is timely and relevant and requires a more agile and flexible approach. Cyberspace Operations, IT Services, Information Assurance/Cybersecurity, and Architecture can no longer be treated as stovepipe policy issues if the Air Force is to maintain its cyberspace operational advantage.

**Vector:** SAF/CIO A6 will continue to increase the agility of its policy approach, to include writing interim changes as soon as an AFI or AFMAN is published. This approach allows for active involvement and feedback from all stakeholders at four to six month intervals. Rapid response to policy changes and updates will provide the Cyber-Airmen in the field the guidance needed to successfully support, execute, and enhance Air Force core missions. Policy will reflect the Information Dominance Flight Plan tenets and drive necessary change. For example, the transition to JIE, cloud computing, and Defense Enterprise E-mail will be partially enabled through the tasks as well as the roles and responsibilities directed in policy. Policy will direct how the Air Force will conduct cyberspace portfolio management, architecture, and governance and we will treat policy as a single portfolio that drives unity of effort.

**Action:** SAF/CIO A6 is charged to foster the flow and sharing of information across mission processes and systems to improve warfighter effectiveness and foster operational successes across all mission areas. To clearly codify the roles and responsibilities in cyberspace the Air Force will transform the current outdated policy framework. This includes transforming information and information systems policy through the creation of a new 17-series of publications by 4Q FY16 (IDFP Objective 4.1). All cyberspace policy currently residing in 10-17 and 33 series policy will be consolidated in a new 17 series, matching the Cyberspace Operations career field AFSC. Information Management programs that fall under SAF/CIO A6 purview will remain under the 33-series of publications. SAF/CIO A6 will also review and update, at a minimum, the following policies:

AFPD 33-4, *Information Technology Governance*  
AFPD 33-1, *Cyberspace Support*



AFI 33-401, *Air Force Architecting*  
AFPD 33-5, *Warfighting Integration*

The cyberspace/IT community will update additional AFIs and official documents as needed and determine whether additional policies are required to align with DoDD 5144.02. This review will include working with AF/A5/8 and SAF/AQI to review and update AFPD 90-11 and AFI 90-1101 to formalize SAF/CIO A6's Title 10 U.S.C. § 2223 role for budget review within existing Air Force Corporate Processes.

---

## Enterprise Architecture

Enterprise architecture is the “explicit description and documentation of the current and desired relationships among business and management processes and information technology.”<sup>50</sup> Enterprise architectures provide several benefits to support warfighting capabilities:

1. Serve as a force multiplier for C2 through effective interoperable capabilities for joint warfighting
2. Improve communication among and between CCMDs, Services, Agencies, MAJCOMs, and Functional Components
3. Drive planning and decision-making by capturing and organizing facts about the mission and functions in a consistent and understandable manner
4. Support analyses of alternatives, risks, and trade-offs
5. Provide structure for requirements documentation

The Air Force Enterprise Architecture (AFEA) is a strategic information resource that documents the capabilities of the Air Force in terms of its people, processes, and technology and relates those capabilities to the Air Force core missions and strategic vision. The Air Force requires architectures to support decision-making about IT investments and manage the complex systems within the cyberspace domain to increase cybersecurity and core mission effectiveness.

A key component of the enterprise architecture is the Consolidated Enterprise Information Technology (CEIT) initiative: the Target Baseline/Implementation Baseline/Operational Baseline (TB/IB/OB) construct. This initiative is an enabler, specifying the technical direction provided in the Information Dominance Flight Plan and Mission Area Annexes and is critical to

---

<sup>50</sup> DoDI 8330.01, 21 May 2014



manage costs, increase agility, and improve cybersecurity. Each baseline is described below:

1. The Target Baseline (TB) specifies the standards, protocols, and guidance for the future state of the Air Force IT infrastructure.
2. The Implementation Baseline (IB) is the baseline of “in-pipeline”/planned products and their TB-informed/allowed configurations that implement the architecture, standards, and protocols specified in the TB.
3. The Operational Baseline (OB) is the set of IB components appropriately configured and deployed across the Air Force’s IT infrastructure to provide the point of departure for required warfighter capabilities and performance.

**Challenge:** Multiple stakeholders and users within the DoD enterprise create complexity in designing and implementing cyberspace capabilities. Not only are current missions placing an ever increasing focus on the requirement to interoperate with Joint and Coalition partners but even the individual platforms within the Air Force face an ever-increasing requirement to fully play their part in enabling net centricity across the operational domain. The Air Force lacks a relevant and accessible enterprise architecture to address complex relationships across mission areas. The enterprise architecture contains information on the current "as-is" state and a future "to-be" state. The as-is state reflects decisions already made and will provide the basis for future decisions addressing how the Air Force is organized, how it performs its mission, the information exchanges, and the systems and technologies it uses. The Air Force is now challenged with building and sustaining an enterprise architecture that will support a growing number of systems and users.

**Vector:** The Air Force will develop an enterprise architecture for the approved, prioritized “as is” and “to be” portions of the system. Properly resourcing the development and sustainment of the AFEA, to include its compliance with established standards, is critical in ensuring alignment of multiple architecture development efforts throughout the Air Force. The Air Force will enable the development of architectures that directly support and are responsive to decision makers across mission areas. All subordinate architectures will be consistent with the AFEA to support the following requirements:

1. Facilitate mission area management, including IT portfolio management
2. Deliver guidance and context for new architectures
3. Increase mission effectiveness through rapid interruption of the cyber kill-chain
4. Provide AFEA information to satisfy CIO concerns; e.g., cybersecurity
5. Enable statutorily-required compliance assessments; e.g., interoperability



**Action:** The Air Force will develop and use the AFEA to guide investment strategies and establish the Architecture Executive Committee to govern initiatives as well as update Air Force architecture policy to guide the development and use of architecture NLT 4Q FY16.

---

## Cybersecurity

**Challenge:** Cybersecurity is a critical enabler to the proper execution of Air Force core missions. The persistent and evolving cyberspace threat necessitates a broad risk management approach that encompasses people, culture, and operational and security engineering processes that will improve mission assurance. In an environment where functionality and security are competing priorities when developing modern information, security-related functions are often traded for performance, forcing security engineers to design and build systems with some level of risk.<sup>51</sup> Cybersecurity of our systems needs to be understood and designed in throughout so that system designer can make the most informed security-related decisions and mitigate risk to our most critical weapons systems. As a result, the Air Force must take the right steps toward implementing cybersecurity throughout weapon systems development and program management, focusing efforts to secure information for core missions and reduce security related risk.



**Vector:** Four lines of effort outline the Air Force focus on cybersecurity

1. Further develop and implement education and training programs to raise awareness of cybersecurity threats to core missions – this includes educating and informing all Airmen and industry partners on how malicious software (malware) can infest mission/weapon systems platforms. Prevention and education is crucial to achieve lasting success and change in Air Force culture and how we address cybersecurity. This line of effort will focus on ensuring all Airmen not only get the right training, but also the supportive intelligence information to make the right decisions.
2. Utilize and influence the acquisition process to enable and implement "Cyber Secure" mission/weapon systems design, engineering, and testing with experienced cyber professionals. This includes updates to the acquisition processes to ensure early engagement and effective system security engineering from the earliest stages of development will "bake in" cybersecurity. A critical enabler for this effort is ensuring experienced Cyber-Airmen are integrated in key acquisition assignments. Overhauling

<sup>51</sup> Evans, H., Heinbuch, D., Piorkowski, J., & Wallner, J (Nov-Dec 2004). Risk-based systems security engineering: Stopping attacks with intention. *Security & Privacy, IEEE*, 2 (6), 59-62.



the certification process and transitioning to the risk management framework will also play a key role in institutionalizing an effective long term risk management process.

3. Focus cybersecurity operations for weapon systems and Program Management Offices (PMOs). This will be done by operationalizing cybersecurity from Air Force Space Command (AFSPC)/24th Air Force (24 AF) to mission systems and weapons systems owners beyond the Air Force Network (AFNET). To do this, an effective process will be established where Air Force Material Command (AFMC) and the acquisition community work with operational commanders to ensure current and future mission systems, weapons systems, functional systems, and maintenance systems will incorporate cybersecurity basics.
4. Establish accountability and ownership of cybersecurity from the cubicle to the flight line. Ensuring effective cybersecurity is everyone's job - the ultimate goal is to ensure our culture changes to accept and implement that concept.

Cybersecurity encompasses all cyberspace and IT activities. As cyberspace assets are continually vulnerable to adversarial attacks, the Air Force requires a plan to improve and maintain the security of cyberspace systems across the Air Force enterprise. For each objective outlined in the flight plan, there are specific and actionable tasks necessary in meeting cybersecurity requirements. The 2015 Cybersecurity Plan provides the detailed tasks for action associated with each flight plan objective and serves as the Air Forces' documented program to focus Air Force efforts. The Cybersecurity Plan directly aligns with the Information Dominance Flight Plan and serves as the way ahead for the A6 community to reach its desired end state with respect to cybersecurity and mission assurance.

**Action:** To support the risk management process, SAF/CIO A6 will update AFI 33-200 and AFI 33-210 to reflect the new Risk Management Framework certification process by 4Q FY15 as well as make recommendations to amend the cybersecurity Assessment & Authorization process to include a new risk management framework process NLT 4Q FY16. To implement cybersecurity throughout weapon systems development, the Air Force will: 1) improve dissemination and develop penetration metrics for DAMO and DIB reports and analytics to facilitate corrective actions for Air Force missions by 1Q FY16; and 2) test new cryptographic technologies within one year of market availability for applicability and modernization of Air Force use.



## Task Force Cyber Secure

**Challenge:** Cyber vulnerabilities have shifted from the traditional “network” attacks (e.g. AFNET, NIPRNET, SIPRNET) to core mission systems, weapon systems, and industrial control systems. There is currently no single Air Force enterprise in place to manage cybersecurity for these systems, thus leaving them vulnerable to exploitation or attack. Although there are multiple well-intentioned efforts underway to address cybersecurity within individual domains, the AF lacks a holistic strategy in defending these assets; the result is ineffective cyberspace defenses that could hinder execution of Air Force core missions. Additionally, the Air Force lacks a holistic approach in performing cyber vulnerability assessments on existing mission, weapon, and industrial control systems.



**Vector:** The Air Force requires an enterprise approach to prioritize, synchronize, and coordinate mission assurance activities of its core missions. The Air Force will establish a Task Force to synchronize the multiple efforts and studies addressing cybersecurity across the Air Force as well as implement an operational focus to increase the robustness and resilience of core mission systems. An operational focus will synchronize efforts from a full enterprise perspective and also develop recommendations that will lead to corrective actions.

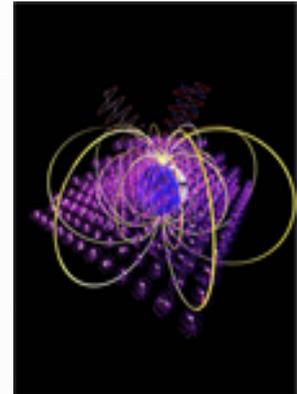
**Action:** AF/A2, AF/A3, SAF/AQ, and SAF CIO/A6 will establish and lead a one-year Cybersecurity and Operations Task Force to develop recommendations and a roadmap to enhance and enable the warfighter’s ability to execute Air Force core missions in and through cyberspace by 4Q FY16.<sup>52</sup> Upon completion, The Task Force will deliver the CSAF an “Air Force Core Mission Cybersecurity Posture 2015” report which will include results and recommendations for synchronized and prioritized cybersecurity investments for future planning.

<sup>52</sup> Cybersecurity Task Force kick-off date is April 2015.



## Spectrum

**Challenge:** The increasing complexity of military systems and the demand for more and timely information is causing an increase in the DoD's need for spectrum management. Electromagnetic Spectrum (EMS) is a prerequisite for modern military operations. The 2013 DoD Electromagnetic Spectrum Strategy states that adversaries continue to aggressively field electronic and cyberspace technologies that impede military operations. Additionally, as the growing wireless broadband industry seeks to reallocate spectrum from defense users to commercial users to meet growing consumer demands for greater mobility and better data access, it is incumbent upon the Air Force to address the future of ensure access to the congested and contested electromagnetic spectrum through close collaboration with spectrum regulators to ensure efficient, flexible, adaptable, and agile capabilities are authorized for use. Through agility, the Air Force can enable DoD systems to better achieve mission success in the rapidly changing electromagnetic environment.<sup>53</sup>



**Vector:** Mission success of Air Force core missions is dependent on reliable access to the electromagnetic spectrum; this success relies on the ability for service components to assemble mission-tailored capabilities with compatible systems to meet CCDR requirements.<sup>54</sup> In realizing these improvements, DoD systems will be more efficient, flexible, adaptable, and spectrum operations will become more agile in their ability to access the spectrum across all domains. To meet these requirements, the Air Force will modernize Spectrum Management to ensure trusted and reliable interoperability among component mission systems and develop spectrum-dependent systems that a more spectrally efficient, flexible, and adaptable within the information environment. The Air Force will be able to meet the air component commander's requirements and trust that systems will be interoperable with each other and be able to adapt to a dynamic environment. The Joint Electromagnetic Spectrum Operations (JEMSO) CONOPS, once published, will define the Air Force approach for managing spectrum in future conflicts. The Air Force will in conjunction with the Sister Services in improving spectrum-dependent capabilities while increasing the warfighter's capacity to operate in the complex spectrum environment.<sup>55</sup>

**Action:** The Air Force will modernize AF Spectrum Management process IAW Joint Electromagnetic Spectrum Operations CONOPS, including adopting the DoD Spectrum Management System by FY17.

<sup>53</sup> 2013 Electromagnetic Spectrum Strategy.

<sup>54</sup> Ibid.

<sup>55</sup> Ibid.



## Force Development

**Challenge:** The Air Force faces challenges in building the highly skilled and trained technical force need to conduct effective cyberspace/IT operations. Competition for human resources with private industry and the commercial sector is high, making it difficult to develop and retain Airmen with Science, Technology, Engineering, and Mathematics (STEM) degrees and technical expertise. Expansion of cyberspace/IT skillsets, to include knowledge of commercial, public, and military networks



employed by partner nations and adversaries is necessary to successfully accomplish air, space, and cyberspace operations including: integrated air defense systems, command and control, supervisory control and data acquisition, space, and airborne networks.

**Vector:** The Air Force will recruit individuals with the required skillsets of academics, experience, and aptitude to provide the foundations for success as Cyber-Airmen. These foundational skillsets will be bolstered through continual education (schoolhouse and professional military education) and employment within units that focus on technical and Air Force core mission competencies driving integration of cyberspace capabilities. We will sustain and resource those subset of our cyberspace forces to integrate cyberspace effects across the warfighting domain.

The Air Force will deliberately cultivate Cyber-Airmen able to dynamically design, build, engineer, and configure within the information environment, defend friendly capabilities and resources from attack through cyberspace, and plan and execute cyberspace operations integrating air-minded expertise to achieve joint/combined forces commander objectives. Initial Qualification Training (IQT) will provide the system and positional specific training prior to mission qualification.

The Air Force will continue to build its highly skilled civilian workforce through accessions based on mission needs and continuing education and the appropriate certifications necessary to meet mission requirements and foster continuity within the units. This includes access to cyberspace development courses (with appropriate clearance levels) as well as Program Management certifications for IT acquisition personnel. Cyberspace activities will increasingly align with industry. As our architecture modernizes, the Air Force will transition in favor of



increased emphasis on battlefield maneuver (e.g., extension into combat theaters, damage mitigation and vulnerability/attack remediation through tactical and operational engineering, etc.), dynamic configuration/sustainment, defensive, and offensive capability development. Our Cyber-Airmen will have opportunities to cross-flow between organizations and functions operating at the tactical, operational and strategic levels. All Cyber-Airmen will be developed into experts not only in cyberspace, but in the core missions to which they contribute. The Air Force will work toward attracting and retaining recruits with prior cyberspace experience and certification to help develop a more robust cyberspace force.

**Action:** Several actions support the future of cyberspace force development:

1. Improve the workforce by developing a cyber aptitude assessment for augmentation of/inclusion in accession testing by 4Q FY17
2. Implement programs to attract and retain recruits with prior cyber skills, experience, and certification with incentive programs by 4Q FY18
3. Ensure every Cyber-Airmen position in the Air Force has Initial Qualification Training (IQT) associated with it by 4Q FY19
4. Develop and implement a plan for civilians in appropriate cyberspace positions to receive military-equivalent cyberspace training (e.g. Cyber 200/Cyber 300) by 4Q FY18
5. To support the alignment of cyberspace/IT activities with those in industry and to grow the professional IT workforce, the Air Force will develop and implement a plan to certify IT acquisition personnel as Program Managers by 4Q FY19
6. Shorten the timeline for implementing training courses on emerging technologies to 120 days from time the need for the training is identified

---

## Governance

**Challenge:** Governance is the framework of rules and practices that ensures continuity, collaboration, and de-confliction of interests across an organization. The intent of governance is the increase accountability from the highest to lowest levels, build transparency to promote trust, and manage stakeholder interest across the organization. Many governing bodies exist within the Air Force and DoD to manage and oversee activities; however, there are few organized bodies that govern enterprise-wide IT capabilities across the Air Force and fundamental processes required for designing an IT governance process have not been established. Additionally, the lack of continuity and transparency across cyberspace/IT



governing bodies hinders mission accomplishment through increasing project costs, unmitigated risks, schedule delays, and the implementation of low-value mission benefits.

**Vector:** The Air Force will design and implement an effective governance process to build the foundation for IT investment success. The primary governance forum for Air Force Information Dominance issues will be the Information Technology Governance Executive Group/Board (ITGEG/B). A strengthened enterprise cyberspace governance structure will be in place across mission areas to align accomplishment of milestones and reapportion resources as required to meet priorities. This governance will be connected to and aligned with the overarching DoD and Air Force governance structures. All subordinate governance structures will deliver relevant input into the ITGEB. The ITGEB structure will provide leadership and guidance for the strategic planning process, as well as oversight of, and accountability for, implementation activities.

**Action:** SAF/CIO A6 will increase the effectiveness of Enterprise Information Dominance Governance (EIDG) by establishing policy to describe the EIDG structure, roles, and responsibilities and their relationship to the IDFP by 1Q FY16.

---

## Investment

**Challenge:** Effective cyberspace/IT capabilities and systems pose significant resourcing and investment challenges to the Air Force due to the rapid delivery and implementation timeline. In a fiscally constrained environment with multiple programs competing for resources, there is a need for a more organized and governed portfolio management system that can oversee and articulate cyberspace/IT requirements to the appropriate decision-makers within the Air Force. Additionally, the Air Force has historically relied on an ad-hoc approach of unpredictable and un-prioritized criteria or making IT investment decisions that result in increased costs, unmitigated risks, and low-value mission benefits. The Air Force needs a standardized Air Force Portfolio Management (PfM) process to assist in the management of IT investment management.

**Vector:** SAF/CIO A6 will perform programmatic reviews and provide investment guidance through a robust Portfolio Management program. SAF/CIO A6 will provide Cyberspace/IT investment guidance by strengthening governance processes for IT solutions at the enterprise level to maximize interoperability across core mission areas and provide the means for making decisions and recommendations based upon enterprise strategic planning, integrated architectures, and outcome-based performance measures. It will oversee these investments through the entirety of the Portfolio Management and Capital Planning and Investment Control (CPIC) process. An effective portfolio management and governance process will influence investment decisions within existing corporate processes so that the Air Force efficiently



delivers cyberspace/IT solutions effectively meeting core mission needs that are secure and compliant; maximizing assurance of Air Force operations in and through the cyberspace domain.

SAF/CIO A6, through the Portfolio Management and Enterprise Resources and Governance divisions, will continually engage with the HAF Space/Cyberspace Superiority panel, Command and Control (C2) panel, the Space/Cyberspace Core Function Leads (CFL), AFSPC/FMP, SAF/AQ, SAF/US(M), SAF/FM, and AF/A5/8 to identify, and advocate the most critical cyberspace/IT investment requirements for timely submission to the Air Staff Program Objective Memorandum (POM) process. Constant engagement within the PPBE and HAF Corporate processes is needed to ensure SAF/CIO A6 priorities and intent are communicated through the appropriate Air Staff channels.

The Air Force will also develop a CPIC process that will integrate with budget, financial, and program investment decisions IAW DoDI 8115.02 and US Code Title 40 § 11312 to maximize the value of IT investments through assessing and managing risk.

To help the Air Force optimize the effectiveness of investments in cyberspace, SAF/CIO A6 will provide enhanced IT/cyberspace investment guidance by strengthening governance processes<sup>56</sup> and by bringing A6-wide participation to IT solutions at the enterprise level to maximize interoperability across core mission areas. This action will also provide the means for making decisions and recommendations based on enterprise strategic planning, integrated architectures, and outcome-based performance measures. SAF/CIO A6 will oversee these investment activities through compliance with the Clinger-Cohen Act, National Defense Authorization Act, Portfolio Management processes, and the CPIC. These compliance processes will influence investment decisions within existing corporate processes so that the Air Force can deliver IT solutions in an effective and efficient manner and meet core mission needs, thus maximizing mission assurance of Air Force operations in and through the cyberspace.

**Action:** SAF/CIO A6 will conduct several actions to conduct effective cyberspace/IT investment and portfolio management:

1. Improve financial efficiency and warfighting effectiveness by developing and implementing a Capital Planning and Investment Control (CPIC) process for implementation in WMA, DIMA, BMA, and IEMA NLT 4Q FY16
2. Implement a human capital investment strategy to maintain currency of cyber forces NLT 4Q FY16
3. Design the AF IT governance and document CIO governance policies and procedures in

<sup>56</sup> ISO 38500.



a guide, charter, and AFI by 1Q FY16

4. Provide a framework for governing the Information Dominance Flight Plan to include establishing initiatives NLT 1Q FY16
5. Transform IT financial management to implement “End-to-End” plan-spend-performance decision-making NLT 4Q FY17.

---

## Cyberspace Command and Control (C2)

**Challenge:** The Air Force has responsibility to support USCYBERCOM and Combatant Commanders under the Unified Command Plan (UCP); this requires C2 structures through AFCYBER (24 AF) to USCYBERCOM, as well as Service responsibilities through the MAJCOM/NAF to the supported operational joint forces commander (JFC) for operations within the JFC’s area of responsibility (AOR)<sup>57</sup>.



Currently there is not continuity or commonality among the Combatant Commanders for cyberspace C2, thus increasing complexity of operations when developing CONPLANS and CONOPS as well as during exercise execution and deployment operations.

**Vector:** SAF/CIO A6, in coordination with AF/A3, will ensure cyberspace operations C2 constructs are developed that support Service requirements as defined in the UCP; DoDD 5100.01, Functions of the Department of Defense and Its Major Components; and JP 3-12, Cyberspace Operations and other like requirements. This construct will address Service support when USCYBERCOM is the supported command for global cyberspace operations, as well as support to Geographical Combatant Commanders (GCCs) when the GCC is the supported command for cyberspace operations with first order effects within the GCC’s AOR. This will require looking at cyberspace operations C2 at all levels to include AFCYBER, MAJCOM/NAF level within a GCC including MAJCOM/AFFOR Communications Coordination Centers (M/ACCCs) and J/CFACC support, and base-level. Additionally, Service roles under JIE must be addressed to include responsibilities for oversight/C2 of IPN/SPPNs.

**Action:** In collaboration with the other Services, the Air Force will develop an all-inclusive operational cyberspace JIE-aligned C2 construct by 2Q FY16.

---

<sup>57</sup> The 212105ZJUN13 CJCS Execution Order (EXORD): Implement Cyberspace Operations Command and Control (C2) Framework directed implementation of USCYBERCOM’s “Direct Support” C2 Model and a Joint Cyber Center (JCC)/Cyber Support Element (CSE) construct with movement toward USCYBERCOM’s “OPCON C2 Model”. Since June 2013, JIE has grown and now includes the Joint Forces Headquarters – DoDIN (JFHQ-DoDIN) and GEOC/EOC C2 model.



## Initiatives

### Data Center Consolidation

**Challenge:** The evolving technology landscape presents challenges in our ability to effectively harness, manage, and deliver critical information to the warfighter. The DoD has more than 1,000 fixed, non-tactical data centers across the globe ranging from large dedicated sites delivering DoD Enterprise-wide services to installation-level users supporting individual base operations. These data centers were developed around the needs of the parent installation without consideration of interoperability, standardization, efficiency, or the ability to migrate to newer, more advanced technologies. As the successful execution of JIE operations relies upon the establishment of standardized processes and functions<sup>58</sup>, the lack of standardization across data centers creates challenges in assessing the cost of ownership, and also creates unnecessary security risks due to lack of cybersecurity controls. Despite concerted efforts over the past decade to consolidate the network operations on individual bases under the base Network Control Center, the Air Force still has many data centers, each driving facility, energy, technology refresh, security, personnel and licensing costs. The growth in data center infrastructure investments is now unsustainable and drives a fundamental shift in how we deploy technology across our systems.

**Vector:** The Air Force requires a set of highly capable, highly resilient, and standardized enterprise data centers that will deliver an agile and ubiquitous set of computing capabilities as part of the JIE.<sup>59</sup> The shift to a more enterprise-oriented environment will enable joint warfighters with an increased focus on obtaining information for decisions needed to achieve mission objectives. Computing and storage services will be delivered through a network of consolidated data centers that deliver cloud-based, on-demand services while also continuing to support legacy services and applications.<sup>60</sup> Additionally, consolidation will help the Air Force in reducing the overall energy and real estate footprint costs, reduce the cost of hardware and software operations, increase the cybersecurity posture, and shift our IT and cyberspace investments to more efficient computing platforms and technologies.<sup>61</sup> Through data center consolidation, the Air Force will make common applications and services available to all DoD users.

**Action:** The Air Force will rationalize all applications through the Portfolio Management (PfM)/CPIC process, migrate relevant applications to JIE Core Data Centers, and establish Installation Processing Nodes and Special Purpose Processing Nodes IAW JIE standards. The Air Force will transition all Air Force data-centers to the JIE construct (e.g., IPN/cloud) by 4Q

<sup>58</sup> JIE CONOPS, Sep 2014.

<sup>59</sup> Ibid.

<sup>60</sup> Miller, R. (1 Mar 2010). Data Center Knowledge. *Feds Commence Huge Data Center Consolidation*

<sup>61</sup> Ibid.



FY17 (APCs/RDCs to be divested by 4Q FY18).

---

## Data Management

**Challenge:** Data underpins decision-making during peacetime and wartime operations. The analysis and assessment of friendly and enemy activity informs decisions and increases operational effectiveness across the DoD mission areas. The growing number and sophistication of adversaries in cyberspace and the lack of governance in place to manage and exploit data proactively hinders the quality and accessibility of data, undermining operational efficiency, risk mitigation, and the agility of Air Force core capabilities. Providing reliable and useable operational data to warfighters is critical in obtaining the operational advantage inherent in information dominance. Data risk comes in many forms from manipulation or outright theft by adversaries to privacy violations and litigation to target miscalculations and navigation unreliability. A key challenge for the Air Force is gaining the ability to interpret the meaning of the data and then assess best practices for storing, managing, and accessing it to ensure the data can enhance operational effectiveness and provide the warfighters with usable, tangible data at the right place and right time.

Although there are overarching policies within the DoD to capture data for archival purposes, the DoD is staggering under point-to-point integrations of outdated and legacy applications and inconsistent data semantics. Our policies do not provide specific details and processes needed to organize, maintain, and preserve data so that it is viable, accessible, and relevant to authorized users. Although we highlight the need to update our policies, to make the data management strategy executable to users, we need to determine what data management actions should be codified in policy and what actions should be outlined in CIO guidance; this will provide more tangible guidance and clarity in the desired actions and outcomes for data management. These issues drive complexity in addressing data management strategies, ensuring the veracity of data, and supporting warfighter missions across the globe.

An integral part of data management is the sharing of information. Information Sharing is the exchange of data between organizations, people, and technology and provides an effective framework to identify and target vulnerabilities.<sup>62</sup> The proliferation of distributed networks, cross-platform compatibility, application porting, and standardization of IP protocols have all facilitated the growth in information sharing. As a result of the continual transfer of information there is an immediate need to put data into context so it is understandable by decision-makers, provide assurance to users that the shared information can be trusted, make users aware that resources and information are available, provide controlled access to needed information, and promote methods to ensure information is protected.

---

<sup>62</sup> Pelfrey, W.V. (2005). The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats. *Journal of Homeland Security and Emergency Management*, 2(1), 9.



**Vector:** The Air Force needs data management policies and protocol that will enable warfighters to make faster, more informed decisions while at the same time increasing efficiencies, efficacy and security of Air Force mission systems through data characterization. The policies will provide guidance in identifying and prioritizing governance of operational data as well as decrease the likelihood/risk of operational and intelligence data compromises. Updated policy should also direct existing IT governance bodies to establish a common ontology that will define and compartmentalize the type, properties, and interrelationships of data within the cyberspace domain.

An additional key focus area is how the Air Force will measure success through data management. One form of measurement is how quickly we can transfer useable data from the source to the warfighter. To improve the speed of data transfer, we need a combination of the typical engineered and systematic processes associated with IT systems combined with new innovative, adaptive and iterative processes. This bimodal approach affords the opportunity to explore solutions that will produce the measurement tools required to assess our data management practices. For example, we can experiment with practices such as automation and data tagging, but need new insights into how those practices can generate value-added information. By being an agent of change, we are better equipped to ensure our data management approach not only delivers reliable data, but data that generates value for its users.

**Action:** To move toward effective data management, the Air Force will develop a roadmap within the IEMA annex for implementing DoDI 8320.02 data standards by 4Q FY15. To increase the ability to effectively identify useable data, the Air Force will stand up data governance and data distribution architecture communities of interest and will ensure relevant mission area applications/systems are registered in Enterprise Information Technology Data Repository (EITDR) and/or Data Services Environment NLT 4Q FY15. To enhance data protection, the Air Force will also deploy an authentication infrastructure to dynamically control authorized user access to information by 4Q FY19.

---

### Single Security Architecture (SSA)

**Challenge:** The responsibility for network security on installations is currently divided among the services, where each service conducts their own security measures through their own service-specific gateways. The lack of consolidation for network security at joint installations increases the risk of network attacks and hinders oversight for enterprise security operations.

**Vector:** The Air Force will implement a Single Security Architecture (SSA); the SSA is a common cybersecurity architecture linking Global Enterprise Operations Centers and other command and control (C2) nodes that oversee and protect the consolidated data centers and installation processing nodes. Coupled with common operational TTP, the SSA will enable



global and regional situational awareness and a common operational picture of the cybersecurity environment and quick and accurate defensive cyberspace operations from the global to the regional levels. The Air Force will move to a joint-focused architecture with a single ops platform for DCO and DoDIN ops. Joint Regional Security Stacks (JRSS)<sup>63</sup> will serve as the platform to provide DoD-wide boundary protection. The number of security stacks (across all Services) will be reduced from 700 to 25 worldwide

**Action:** The Air Force will establish processes and develop capabilities to protect and defend Air Force information networks and associated systems as a single environment by 4Q FY18 (IDFP Objective 3.4). The Air Force will move to a resilient JIE SSA by replacing all Air Force gateways with a JRSS by 4Q FY17.

---

### Enterprise Operations Center (EOC)

**Challenge:** The integration of IT and cyberspace into Air Force functions and systems has caused Air Force core missions to become more integrated and reliant on cyberspace. This evolution in the Air Force information environment resulted in the need for standardization that is both more cost effective and better able to adapt to emerging technologies. As a result, the Air Force identified the need for the consolidated C2 of networks and information systems to reduce vulnerabilities, increase system resilience, and provide more resource efficient solutions to support information operations and security services.

**Vector:** The Air Force will support the implementation of the JIE EOC to serve as a single entry point and primary executor for DoDIN Ops and Defensive Cyberspace Operations (DCO). The end-state services provided by an EOC will include support to Core Data Centers (CDCs) and assuming operational missions from other EOCs when needed due to failures or outages. The goal is for EOCs to provide computer network defense capabilities to the entire DoD enterprise; this transition will increase security, operational flexibility, and responsiveness. When fully implemented, the EOC will provide combatant commanders reliable situational awareness of DoDIN global operations as well as DCO from a single site, allowing for more flexibility and faster response times to mission requirements.<sup>64</sup>

**Action:** The Air Force will evolve its Network Operations Squadrons to be compliant with JIE EOC standards by 4Q FY19. The Air Force will work collaboratively with DISA to develop and deliver a joint C2/Service desk construct to enable EOC operations NLT 4Q FY17.

---

<sup>63</sup> Joint Regional Security Stack: DoD-wide boundary protection via a single platform – removes the responsibility for network security from the individual, service-specific military installations to an enterprise model in which a small number of centers handle security for an entire region.

<sup>64</sup> Air Force Joint Information Environment Strategy, 2014.



## Aerial Layer Network (ALN)

**Challenge:** Combatant Commanders require multi-layer, high capacity communications networks to employ capabilities across the range of military operations. In support of global operations, the warfighter currently uses a portfolio of tactical data links to exchange information with mission or platform-centric partners; these platforms are limited in capacity and capability and are expensive to upgrade.<sup>65</sup> The insufficient capacity and diversity of existing communication nodes to



provide resiliency and agility for continuity of operations as other communication paths are lost, denied or unavailable, resulted in joint interoperability gaps among aerial, space, and surface communication networks.<sup>66</sup> The Joint Aerial Layer Network (JALN) Initial Capabilities Document highlights the need to close four specific capability gaps with respect to communication networks: network connectivity, network capacity, share information and data, and network management. As airborne networking becomes increasingly important for future forces that will rely on effective communications for mission success, the DoD requires the ability to conduct information sharing among similar, and disparate platforms, provide access to the ground-layer high capacity backbone to extend DoDIN services to tactical edge users, and support Combatant Commanders and national leaders.

The Services face the challenge of integrating aerial layer systems with surface, space, and cyberspace communication assets while resolving interoperability shortcomings. To address this challenge, the Air Force is working to transform requirements, programming, and acquisition processes and policies to increase interoperability in the aerial layer. The way forward is to create a JALN capable of integrating with, extending, and augmenting space, cyberspace, and surface networks to connect and enable the collaboration of warfighters in any joint operations area (JOA).<sup>67</sup>

The JALN, integrated with the space and surface network segments in the JOA, enables advanced warfighter information exchange capabilities that support Air Force core missions. The JALN ensures communications capabilities remain available to the warfighter, even in the most austere environments where adversaries are able to disrupt DoDIN connectivity.<sup>68</sup> The highly contested cyberspace domain requires diverse, accurate, timely, and information-assured access to data, information, intelligence, situational awareness, and indications and warnings at

<sup>65</sup> JALN Strategic Communications Plan, 2014.

<sup>66</sup> JALN Initial Capabilities Document, 2009.

<sup>67</sup> JALN Strategic Communications Plan, 2014.

<sup>68</sup> JALN Initial Capabilities Document, 2009.



all security levels from which planning and decision-making activities can be initiated, executed, and monitored, regardless of the environment – the JALN will enable these cross-cutting capabilities to support Air Force C4ISR operations as well as the C2 operations of the sister services.<sup>69</sup> The JALN will be modular, scalable, and flexible to enable network connectivity among communication nodes and will be highly responsive and available to taskings.<sup>70</sup>

**Vector:** The Air Force will address capability deficiencies in airborne networking to increase effectiveness and decision superiority by integrating with, extending and augmenting space or surface networks to connect, reconnect and enable the collaboration of Joint and coalition warfighters. JALN development, aligned to the Air Force and Joint vision for JIE, is important to extending the JIE architecture and services to the tactical edge. However, our approach to this challenge is not limited to technology development. From modifications to a legacy fleet, to doctrinal incorporation of aircraft networking roles, to the supported and supporting roles within the cyberspace domain, we will continually leverage innate Air Force innovation. The Air Force will coordinate with Sister Services to develop JALN component systems that will enable decision superiority by connecting the right people with the right information at the right time. Communications advancements in the aerial layer network, with the range, customization, and access they can provide to all domains, offer significant opportunity for transformative gains in warfighter effectiveness.

**Action:** Through the corporate process, the Air Force, through the JALN Core Function Lead, will provide strategic direction and investment inputs to ensure airborne networking investments improve warfighting effectiveness across mission areas.

---

### Base-Level Infrastructure

**Challenge:** The Air Force spends close to a billion dollars per year on “wired” base-level IT technology refresh and modifications/extensions of base-level IT infrastructure. The fiber optic networks within and between buildings that support computers, phones, and peripheral/supporting devices are a major cost driver in military construction (MILCON) and in utility costs (power and cooling). In addition, the proliferation of commercial off-the-shelf (COTS) hardware supporting every mission area at the base level has resulted in thousands of devices being fielded across every Air Force base without the proper configurations that allow centralized cyberspace operators and defenders to see and protect them. This condition hampers cyberspace domain situational awareness and drives base-level and enterprise



---

<sup>69</sup> Ibid.

<sup>70</sup> Aerial Sensors and Relays Capability-Based Assessment, 2009.



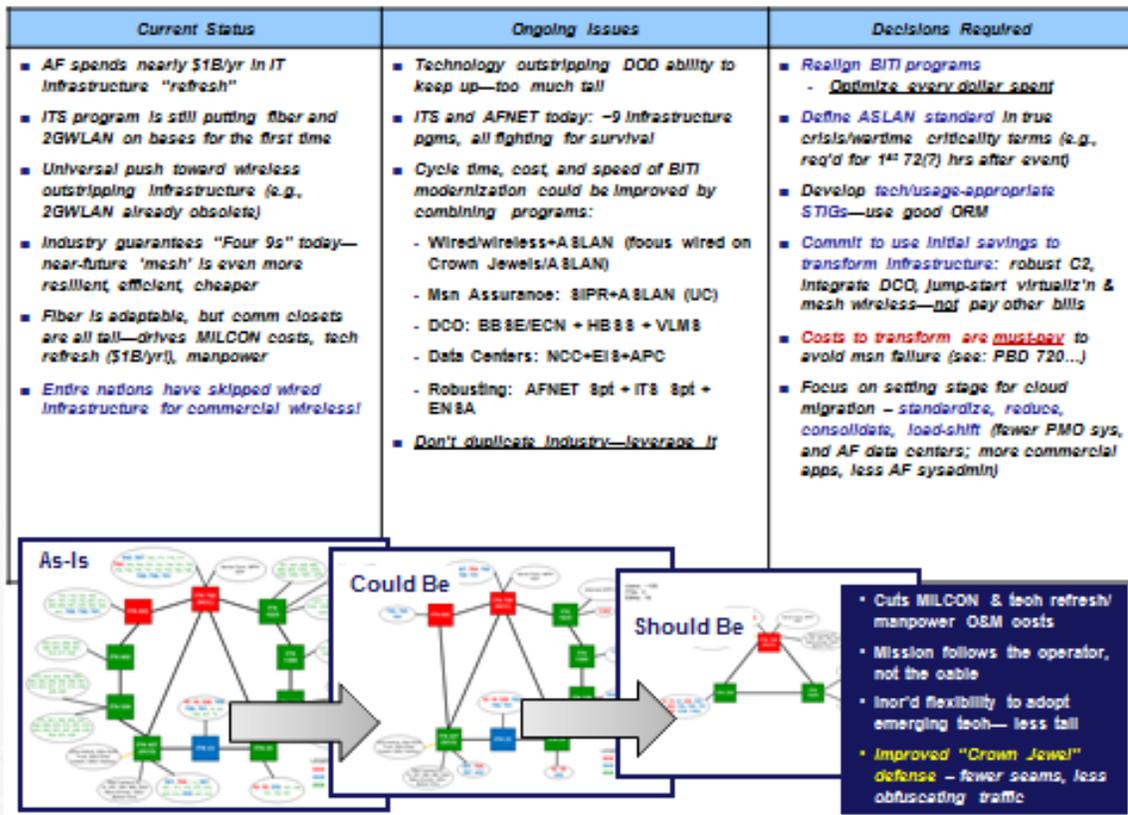
manpower requirements by hindering centralized configuration management actions like software upgrades and vulnerability identification and remediation.

**Vector:** The virtualization of mission and functional systems in a cloud computing environment offers significant opportunities for savings in base-level infrastructure beyond that achieved in data center consolidation. The Air Force will conduct the virtualization of networks and systems to address the cost and the cyberspace defense problems from massive, complex base-level infrastructures. The Air Force will transition most users and applications from wired, fixed computer resources to mobile devices capable of supporting personal, official/administrative, and FOUO/unclassified mission applications via voice, video, or data on a single secure platform. A smartphone in the hands of every Airman is a powerfully transformative direction, allowing our young “digital natives”<sup>71</sup> to proactively leverage commercial applications and ubiquitous information to solve mission problems. The Air Force will reduce base level “wired” infrastructure, focusing resources on implementing and sustaining robust, physically diverse connectivity almost exclusively in support of critical mission assets. Having only mission-critical functions tied to wired infrastructures facilitates the rapid adoption of emerging applications and technologies, and ensures robust backup and continuity of operations capabilities.

Additionally, the Air Force will modernize base infrastructure through an increased focus on IT Lean. IT Lean applies lean manufacturing principles to eliminate IT services and systems that no longer add value to the mission.<sup>72</sup> This approach will move Air Force bases toward commercial wireless services and keep hard-wired systems and services only for those unique, base-specific missions. IT Lean will also help in reducing IT maintenance costs and update cycles while providing reliable IT services across the infrastructure enterprise. Although a continual process, Figure 3 outlines specific decisions that can assist in addressing the ongoing issues associated with current base-level infrastructure. Our ability to consolidate and centralize capabilities and services at bases will not only increase bandwidth and bolster cyber readiness; it will enhance the Air Force’s capability in delivering the reliable and sustainable enterprise services that are essential for mission success.

<sup>71</sup> Prensky, M. (2001). Digital Natives, Digital Immigrants. *On the Horizon* 9 (5): 1-6.

<sup>72</sup> Kindler, N.B., Krishnakanthanm V, & Tinaikar, R. (May 2007). Applying Lean to Application Development. *McKinsey Quarterly*.



**Figure 3. IT Lean Overview**

**Action:** The Air Force will implement a plan to reduce costs by a goal of 10% annually through the rationalization of Air Force applications with a focus on providing Airmen less and better systems to accomplish the mission NLT FY19.

Combat Communications (Extending Services to the Tactical Edge)

**Challenge:** Combat Communications are not sized with modernized equipment to meet current and future Combatant Command, Service and Defense Support to Civil Authorities (DSCA) requirements. Furthermore, Combat Communications are not yet integrated into the JIE.

**Vector:** The Air Force will ensure its deployable cyberspace capabilities are sized, shaped, modernized, and scalable to support Joint, Air Force and DSCA mission





sets<sup>73</sup> in disadvantaged conditions<sup>74</sup> utilizing the JIE. Air Force deployable communications will continue to provide operational commanders the cyberspace capabilities necessary to C2 their assigned forces. The Air Force will also develop plan to migrate deployable Air Force communications directly to JIE by no earlier than the end of FY18 as well as develop a plan to modernize deployable communications equipment to take advantage of survivable technology (i.e. against EMP or satellite jamming [AEHF]) and redundant (i.e. Troposcatter and HF technologies).

**Action:** The Air Force will evaluate the RAND Combat Communications Demand Study NLT end of FY15 and modify Combat Communications force structure as required.

---

### Air Force Installation and Mission Support Center (AFIMSC)

**Challenge:** Limited resources in a constrained fiscal environment require the centralization of core IT services at Air Force installations. Manpower shortages create a strain on mission commanders to effectively execute their core mission sets while providing cyberspace/IT support functions to customers. Additionally, multiple applications and systems across Air Force installations are pulling skilled Cyber-Airmen from supporting the core mission to providing and supporting the more common IT functions (email, knowledge ops) that are not unique to the core mission set.



**Vector:** The Air Force will focus Cyberspace/IT resources on the Air Force core missions themselves and divest Air Force services that can be better provided through the Joint Information Environment. AFIMSC will support bases' long haul communications contracting, IT asset management, engineering, and installation (E&I) plans, and publications management. The resource savings from this consolidation will allow MAJCOMs and mission commanders to refocus on their respective core missions and rely on AFIMSC for those common installation resources.

**Action:** The Air Force, through a phased approach, will consolidate common installation and expeditionary combat support capabilities into a single Air Force Installation and Mission Support Center (AFIMSC). This center will more effectively and efficiently manage common installation resources in today's budget constrained environment. Traditional communication

<sup>73</sup> Mission sets include, but are not limited to, the following: Contingency Response Forces (CRF), Theater Air Control System (TACS), deployable Airfield Operations, Air Expeditionary Wing/Group/Squadron, Combined/Joint Force Air Component Commander (C/JFACC), Special Operations units, and JTF-Civil Support missions.

<sup>74</sup> Disadvantaged conditions include disconnected, intermittent, and low bandwidth conditions as well as deploying and operating in semi-permissive and SATCOM-contested conditions.



and information tasks across every installation will be standardized and centrally executed within AFIMSC. The Air Force, through the Agile Combat Support (ACS), and in concert with the Cyberspace Superiority Core Function Lead (CFL), will plan for and provide POM inputs for AFIMSC core services and manpower requirements. The Air Force will direct the ACS CFL to identify the amount of funding required to support AFIMSC requirements by 2Q FY16.

---

### Senior Leader Communications

The Air Force actively participates in oversight, integration, and advocacy activities for National Leader Communications Capabilities (NLCC) encompassing presidential and senior leader communications. The Air Force also provides representation to the NLCC Executive Management Board. These responsibilities are of such importance to the nation that they require the involvement and coordination of many departments and agencies.

Senior leaders require a continuous and reliable level of Command, Control, and Communications (C3) regardless of their location or environment. The Senior Leadership Command, Control, and Communications System (SLC3S) provides the technological means to U.S. senior leaders through fully converged fixed, deployable, mobile, maritime, and airborne voice, video, and data services via assured communications to enable senior leader C2 in support of national strategic objectives. SLC3S supports the employment of information in the C2 process to coordinate a unified response and execution of critical tactical, operational, and strategic level requirements. The cyberspace operational domain is a key enabler of SLC3S in providing full assured communications/IT capabilities in a wide variety of environments (2012 SLC3S Strategic Guidance).

**Challenge:** Because SLC3S platforms and systems operate in diverse environments and rely upon DoD and non-DoD space, airborne, and ground systems, challenges arise with respect to interoperability and compatibility. SLC3S is dependent upon both military and commercial communication systems to provide connectivity. Competing budget priorities along with systematic acquisition problems have prevented the DoD from implementing an efficient, integrated SLC3S capability. Service components have acquired numerous new systems to address service-specific requirements but have not pursued compatibility across the enterprise or among the users. As a result, several technology-distinct networks and systems have evolved that lack interoperability and collaboration, thus resulting in competing networks that are unable to communicate with each other<sup>75</sup>.

**Vector:** SLC3S will support a variety of capabilities across the range of senior leader's C3 in any operational environment. SLC3S policy will articulate target architectures and TTPs to ensure the effective exchange of information to make and execute decisions. Operational procedures will be updated to reflect the changes and new capabilities will be incorporated into existing

---

<sup>75</sup> SLC3S Strategic Guidance (2007).



processes. The Air Force will work to pursue the technology that fits into the SLC3S architecture to include an enterprise-wide assessment of new technologies for implementation. Interconnectivity between mobile and airborne SLC3S platforms via the GIG and other special purpose nodes is critical in supporting senior leader C2 requirements. Additionally, the Air Force will assess the employment of automated tools that will enhance interoperability and compatibility of SLC3S platforms and systems across the enterprise.

**Action:** The Air Force will upgrade SLC3S communication systems to IP infrastructure as a primary means by 4Q FY19; use link diversity to assure unbroken, survivable communications on specific SLC3S elements.

---

### Position, Navigation, and Timing (PNT)

**Challenge:** Access to PNT information is essential to the execution and command and control of Air Force missions as well as to the efficient operation and protection of information networks necessary for continuous situational awareness by Combatant Commanders and Air Force senior leaders. Air Force PNT has multiple dependencies and systems to include; while the Global Positioning System (GPS) satellite constellation is the cornerstone provider of PNT for the foreseeable future, assured PNT requires a system of systems to complement and provide alternatives to GPS in a defined architecture – this also includes compliance with Precise Time and Time Interval (PTTI) and Navigation Warfare (NAVWAR).<sup>76</sup> As all modern combat weapon and support systems use information in some way, the importance of precise time and precise frequency is growing. The increased vulnerabilities of Air Force systems present risk to operational effectiveness, to include exploitation from adversaries. The fact that critical Air Force systems are at risk for jamming and/or hacking through the denial or degradation of PNT requires the Air Force to take the necessary actions to assure critical data cannot be compromised.<sup>77</sup>



**Vector:** Per DoDI 4650.05, the Air Force, along with the other Services, is required to accomplish several PNT-related key activities that will provide inter- and intra-Service and allied coalition commonality, while leveraging commercial technologies to the maximum extent possible. This includes the development and acquisition of 1) PNT equipment that provides protection against adversary disruption; 2) capabilities to identify, locate, and mitigate interference that affects the use of GPS for military operations; and 3) capabilities to deny PNT to adversaries without unduly disrupting civil or commercial use outside of an area of operations. With the growing

---

<sup>76</sup> DoDI 4650.05, 19 Feb 2008.

<sup>77</sup> Precise Time and Time Interval Management Working Group Charter, 20 Dec 2012.



importance of the PNT enterprise within the DoD, it is incumbent upon the Air Force CIO to support and help shape future policy, investment, and strategy discussions, especially with respect to information networks and protocols.

**Action:** In collaboration with AF/A3 and SAF/AQ, SAF/CIO A6 will support the development of a plan to optimize, align, and support Air Force CIO equities in PNT Enterprise Management and Integration by 4Q FY16.

---

## Cyberspace Capability Development and Innovation

**Challenge:** Growing vulnerabilities in Air Force mission systems require continual investments in capability development to eliminate threats and mitigate negative impacts on systems across the operational domain. Advanced developments in operational cyberspace capabilities are needed to engage key adversary targets and create the effects necessary to deny, degrade, disrupt, destroy or deceive these systems or the data residing on them in support of the Combatant Commander. Cyberspace operations rely on the full range of traditional military operations to be conducted under Title 10 (military operations), Title 32 (National Guard), Title 50 (war and national defense), and authorities and subject to rules of engagement. With their global reach and potentially strategic effects, these activities are a natural extension of Air-minded contributions to joint/combined operations and national defense. In particular, the Air Force's cyberspace capabilities are informed by experience and training, bringing particular focus and emphasis on mission sets such as counter-air, IADS suppression, C2, and counter-space.



Cyberspace operations, presents a continuum of activities, unified by centralized C2, established supported/supporting relationships, and validated TTPs. Military networks and systems will come under attack in cyberspace during the earliest phases of hostilities – perhaps as the first indication of hostilities – so the Air Force will continue the seamless merger of DoDIN Ops and DCO. Additionally, effective management of IT requires significant risk mitigation strategies while ensuring the reliability of data in all domains. The need for the Air Force to reach higher level of maturity in IT and cyberspace technologies is becoming increasingly urgent.

**Vector:** The Air Force will continue to foster relationships with industry, academia, research and development activities, and our national and international partners to invest in the most advanced tools and non-materiel capabilities available for leading edge DCO, Offensive



Cyberspace Operations (OCO), Cyberspace ISR and DoDIN Ops to create the conditions for Air Force core mission execution wherever and whenever needed. The Air Force will explore development concepts to support the future of commercial IT capabilities to include quantum computing, desktop virtualization, digital asset management, homomorphic encryption, software-defined networking, and other applications to streamline network functions and processes. The Air Force will also establish/designate a Cyberspace Innovation Center (CIC) to identify, prioritize, fund, and implement information and cyberspace capabilities through partnerships with academic and public and private research partners. The CIC will provide a centralized environment where Airmen can work hand-in-hand with industry, academia, and agency partners to continually push the leading edge of technology and its applications and create the conditions for Air Force core mission execution wherever and whenever needed. The CIC will be anchored at USAFA and will be chaired by an advisory board comprised of SAF/CIO A6, AF/ST, USAFA, AU, AFSPC, AETC, 24 AF, 25AF, and AFRL. The CIC will be resourced from Air Force and private sources.

**Action:** The Air Force will designate a Cyberspace Innovation Center to identify, vet, fund, and implement information and cyberspace innovations to increase the Air Force's competitive advantages in its core missions. IOC by 4Q FY16

---

## Partnerships

**Challenge:** The rapid growth of cyberspace/IT capabilities poses significant challenges to the Air Force in being able to develop, build, and field timely and relevant systems and capabilities. IT has become a major factor in the ability to enable services and systems in both the government and private sector. How we manage the utility of IT impacts the efficiency and effectiveness of our core missions. The private sector also understands the criticality of technology to act not only as an enabler to create better and faster services, but also how technology can be a facilitator between government and private partnerships.<sup>78</sup> The emerging cyberspace domain requires new and innovative approaches, and government and private sector leaders are beginning to strengthen cooperation and collaboration efforts to capitalize on emerging technologies.<sup>79</sup> In this light, the Air Force requires collaboration and cooperation with outside partners to keep up with the rapid nature of cyberspace and deliver the most effective IT/cyberspace capabilities to the warfighter.

**Vector:** The Air Force will remain closely partnered with the commercial sector, other government entities, and allies in cyberspace. The Air Force will expand the close relationships with interagency partners, including law enforcement and the intelligence community, to identify and pursue threats to the enterprise. We will pursue expanded cyberspace situational

---

<sup>78</sup> *Keys to Collaboration: Building Effective Public-Private Partnerships*, National Association of State Chief Information Officers Corporate Leadership Council, Issue Brief, May 2006.

<sup>79</sup> *Ibid.*



and predictive threat awareness through increased information sharing with public, private, and allies. Creating and further developing these relationships will contribute to a robust, secure enterprise architecture, effective threat awareness, and resilient, flexible defense for Air Force core mission success.

**Action:** The Air Force will develop an action plan to enable information sharing, strategic partnerships, and collaborative agreements (to include a multi-level security capability for cross-domain information sharing) with industry and other partners by 1Q FY17 and plan for implementation NLT 4Q FY18.

---

## Acquisition Reform

**Challenge:** The ability of the acquisition process to deliver cyberspace/IT systems within predicted cost and schedule is not meeting the current demand and need for these systems. New practices are required within the Program Management Offices to ensure systems are delivered in a timely manner to meet warfighter and performance requirements. According to the Senate Armed Services Committee, the acquisition of information technology is a challenge across the DoD and acquisition reform remains a priority.<sup>80</sup> The proliferation of COTS within cyberspace/IT hinders effective control and management and we often seek the most inexpensive solution vice the solution that is most effective.

**Vector:** The Air Force will design and implement common infrastructures and platforms that support multiple systems while minimizing program-unique platforms. By driving the use of standard platforms, we will minimize the number of software upgrades, hardware, and applications required to support such systems, thus reducing the stress of the acquisition process. The Air Force will enable agile IT through the delivery of usable capabilities, active user involvement to prioritize requirements, leveraging common infrastructure platforms, standards, automated tools, and interfaces, and leveraging existing contract vehicles for rapid Task/Delivery Order execution. Cybersecurity will also be incorporated throughout this process. Additionally, we will strengthen IT governance by streamlining compliance processes and ensure IT governance board have an Enterprise view to accurately prioritize IT technologies, investments, and capabilities. Working within acquisition laws, we will work with vendors to find the most effective procurement solutions at the best possible price and schedule to include pursuing “as-a-Service” models. These constructs have the ability to provide rapid deployment, limited infrastructure investment, enhanced levels of service and security, and increased scalability and integration while lowering costs.

**Action:** In collaboration with SAF/AQ and PMOs, SAF/CIO A6 will develop a plan to improve

---

<sup>80</sup> McCain ready to tackle cyber threats, Cost-Plus contracts as a SASC Chairman (3 Dec 2014). *Defense News*. Retrieved from <http://archive.defensenews.com/article/M5/20141203/CONGRESSWATCH/312030041/>.



cybersecurity implementation and cybersecurity test capability, as well as reduce procurement hurdles through effective development of policy that addresses effective IT/cyberspace acquisition processes, Risk Management Framework, and Authorizing Official guidance NLT 1Q FY16. Additionally, SAF/CIO A6 will work to increase agility in responding to the cybersecurity and technological operational requirements (through collaboration and cooperation with SAF/AQ) by ensuring key systems are designed, engineered, tested, acquired, and sustained smartly and efficiently and streamline the IT acquisition process NLT 1Q FY16.



## SUMMARY

As stated in *America's Air Force: A Call to the Future*, one of the most important responsibilities of a military service is to prepare the force for the challenges of tomorrow, not just the realities of today. The Information Dominance Flight Plan prepare for these challenges by outlining the Air Force path for achieving the desired end state in the Information Dominance Vision: *The Air Force fully exploits the man-made domain of cyberspace to execute, enhance, and support its core missions*. The Flight Plan strengthens the Air Force's contributions to defense and sovereignty, helping our contributions remain fully realized in and through an increasingly congested and contested cyberspace domain



Three tenets of Information Dominance guide the flight plan, through effectiveness, security, and efficiencies and innovation. Supporting the vision and tenets, four goals provide the basis for achieving the strategic end state, not only for today, but into the future despite an austere budgetary and rapidly changing security environment. These goals are soundly based, and fully aligned with the Air Force's five core missions as well as the Air Force Strategic Master Plan. They integrate and link operations within the cyberspace domain and information environment back to the Air Force vision and also articulate how SAF/CIO A6 supports the larger Air Force mission.

Of course we will remain prepared to continuously adjust to meet not only emerging threats and demands, but also the changing technological environment around us. We will be innovative, and will understand the warfighters' needs while providing an environment where we maximize use of the global commons to our advantage. The Air Force is steeped in innovation, and we will be bold in how we shape operations in and through cyberspace. Our highly-qualified Cyber-Airmen will enable the application of Global Vigilance - Global Reach - Global Power for America; we will remain unparalleled in our ability to Fly, Fight, and Win in Air, Space, and Cyberspace.