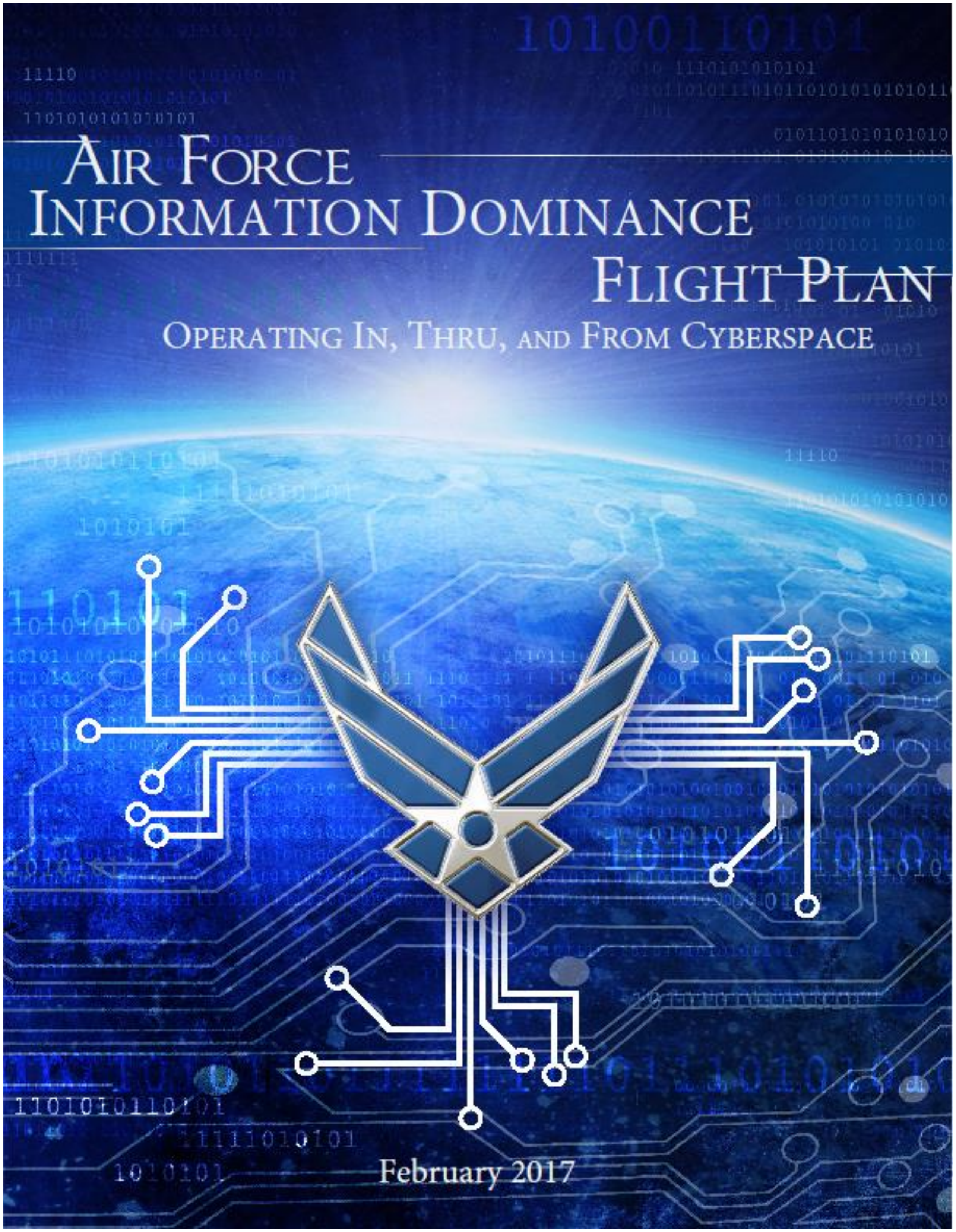


Air Force Information Dominance Flight Plan

Operating In, Thru, and From Cyberspace

February 2017

FOREWORD

This Information Dominance Flight Plan (IDFP) provides the overarching guidance and processes for unifying Air Force cyberspace initiatives over the next 10-years, and it is built on the foundation of the Air Force's Strategic Master Plan and Future Operating Concept to ensure unity of action and effort toward fully exploiting cyberspace. The goals nested herein should influence all aspects of Air Force core missions that leverage cyberspace. To achieve these goals we have incorporated the CSAF's Cyberspace 10-year Targets to unify Air Force Information Dominance lines of effort for guiding our operations in, thru, and from cyberspace.[1]

The Air Force continues to shift from primarily building, protecting, and defending the network, to a convergence of integrated efforts in, thru, and from cyberspace to execute core missions. Our emphasis is toward functioning and fighting as cyber warriors, defending our networks and core missions from attacks, and preparing for offensive operations to execute when appropriate authorities direct. Achieving mission success requires treating data as an asset and incorporating actions to conduct information-age warfare. The Air Force will establish a Chief Data Office with requisite authority to develop policy, implement cross-enterprise governance structures, and grow cross-classification data analytic capabilities.

As the DoD moves from a "culture of compliance to a culture of risk assessment,"[2] and risk management, the Air Force will synchronize information technology investments with mission capability needs focused on mission assurance. Although we will not completely divest network provisioning required to enable core missions, we will make resourcing choices that better leverage government and private sector innovative solutions. These choices will free-up manpower resources enabling a more direct focus on active mission defense throughout cyberspace.

In addition to investing in information dominance capabilities, we will recruit and retain Airmen with cyber and data analytics talent through modern accessions, training, and retention methodologies used in the private sector. Through innovative means, we will evaluate and entice workforce talent; create opportunities to incorporate "non-traditional" talent; and support alternatives for retention of Airmen with mission critical skills.

The Air Force recognizes the symbiotic relationship between warfighter operations and cyberspace, as reflected in increased Future Years Defense Programs (FYDP) investments advancing both defensive and offensive initiatives. However, the traditional model for acquiring warfighting capabilities, particularly cyberspace capabilities, lacks agility in countering adversarial innovation and investments. The dynamic nature of cyberspace requires an

[1] The Air Force established 10-year targets to guide Air Force efforts to operate in, thru, and from cyberspace: situational awareness; mission execution; power projection; mission generation; enterprise services (C4); ISR in cyber; agile acquisition; and warfighting integration. Memorandum *Operating In, Thru, and From Cyberspace*. 29 Jun 2016.

[2] Department of Defense Information Technology Environment. Aug. 2016. http://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf

acquisition process that quickly leverages innovative information technologies and private sector developments. To that end, we will work to leverage agile acquisition programs to meet mission requirements.

Three areas of focus underpin this Flight Plan: first, synchronizing cyberspace efforts across Air Force functional communities; second, unifying and accelerating Air Force cyberspace efforts that outpace our adversaries; and third, fully exploiting cyberspace for our Air Force. Achieving Information Dominance requires leveraging cyberspace to create effects while simultaneously ensuring the domain enables Air Force core missions. We will achieve success through four Information Dominance Strategic Goals:

1. **Assure freedom of action and deliver combat effects in, thru, and from cyberspace to advance the Air Force core missions**
2. **Provide Airmen trusted information when and where they need it**
3. **Organize the cyber workforce, and train and educate all Airmen to utilize the cyberspace domain to accomplish the Air Force missions**
4. **Optimize the planning, resourcing, and acquisition requirements, of cyberspace investments**

Innovation, opportunity and forward-thinking hallmark our Air Force's success. As we look at the Cyberspace Domain, we will be bold information technology investors who shape operations in, thru, and from cyberspace toward Global Vigilance – Global Reach – Global Power for America.

Dash

DASH JAMIESON, Lt Gen, USAF
Deputy Chief of Staff, Intelligence,
Surveillance and Reconnaissance
and Head of the AF IC Element

Mark C Nowland

MARK C. NOWLAND, Lt Gen, USAF
Deputy Chief of Staff, Operations

William J Bender

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

TABLE OF CONTENTS

STRATEGIC FRAMEWORK

As defined in the 2015 DoD cyberspace strategy,[3] the Air Force will work in concert with other federal agencies, the private sector, and international partners to build cyberspace capabilities quickly and efficiently to defend the United States and its interests. This IDFP aligns with this strategy and serves as a unified approach to assuring Air Force core missions.

The DoD has three cornerstone efforts to address the challenges of operating, securing, and defending the cyberspace domain. These three cornerstone efforts are US Cyber Command's (USCYBERCOM) Cyber Mission Force (CMF), the DoD Chief Information Officer's Joint Information Environment (JIE), and the Secretary of Defense's imperative on resiliency of critical capabilities.[4]

In September 2015, the Air Force published the Air Force Future Operating Concept (AFFOC) which broadly portrays how the Air Force will conduct its five core missions in a 2035 operating environment. The central idea is multi-domain operational agility: "the ability to rapidly generate, and shift among multiple solutions for a given challenge."[5] Cyberspace is a key component of the future operating environment which is dynamic and global and requires a unified Air Force to be innovative in developing our weapon systems.

Air Force forces *fly, fight and win… in air, space and cyberspace.* The Air Force protects and preserves our national security interests and offers freedom of action to the Joint warfighter by integrating capabilities to provide Global Vigilance, Global Reach, and Global Power through its five core missions. The AFFOC describes how AF forces will evolve and conduct their core missions in the future: Multi-Domain Command & Control (MDC2); Adaptive Domain Control (ADC); Global Integrated Intelligence, Surveillance, & Reconnaissance (GIISR); Rapid Global Mobility (RGM); and Global Precision Strike (GPS).[6] The IDFP outlines a vision toward assuring the five core missions while achieving freedom of action in, thru, and from cyberspace. It also identifies new requirements such as the establishment of an Air Force Chief Data Office with requisite authorities necessary to achieve IDFP goals and evolve Air Force capabilities needed to conduct information-age warfare. These efforts require trained Airmen who understand how information dominance enables, impacts, supports, and delivers warfighting capabilities through an agile acquisition and governance processes that rapidly integrates needed warfighting capabilities.

Leveraging the Air Force Strategy, Planning and Programming Process (SP3), the IDFP defines strategic future-states for Air Force cyberspace over the next 10 years and describes conditions necessary to achieve these states in relation to the Air Force's Strategic Master Plan (SMP) (Annex-1). The four IDFP goals, in concert with changing objectives are measured through the Air Force governance process using a Scorecard approach detailed below in *Measuring Success*. Figure-1 shows how Air Force strategic documents establish strategic goals to guide Air Force functional communities toward a set of common strategic objectives. The IDFP was developed in alignment

[3] Department of Defense Cyber Strategy, Apr. 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[4] Ibid (pages 4, 6 & 13).

[5] Air Force Future Operating Concept (AFFOC), Sep 2015.

[6] Air Force Future Operating Concept (AFFOC), Sep 2015.

with AF strategic documents and is being implemented in coordinated with all the Air Force Core Function Support Plans (CFSP), especially the Cyber Core Function Lead CFSP.

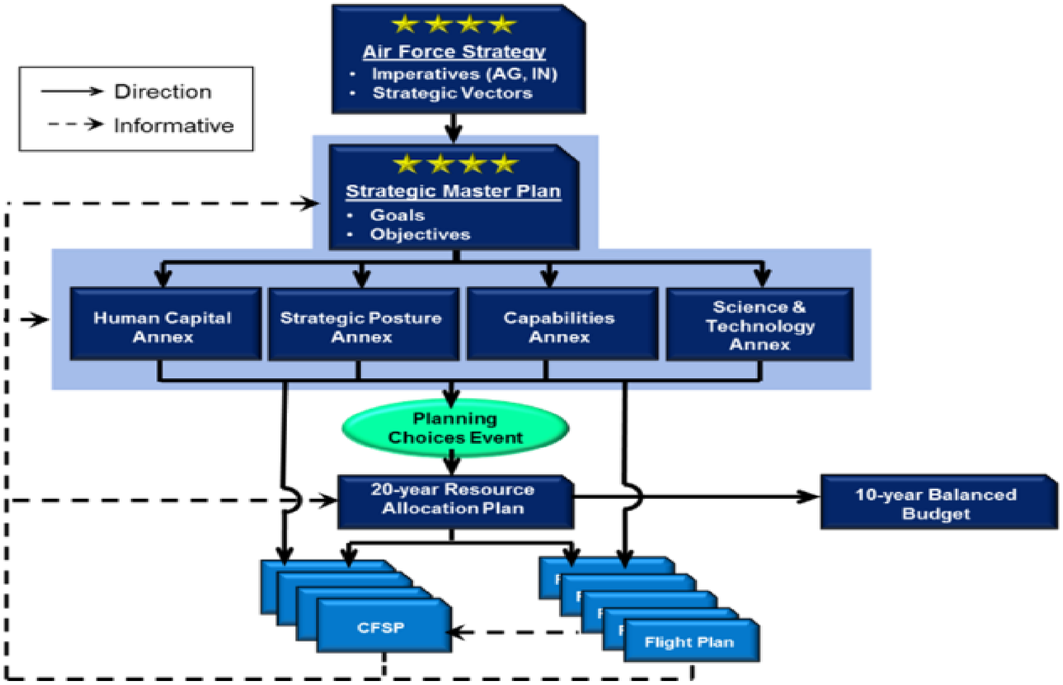
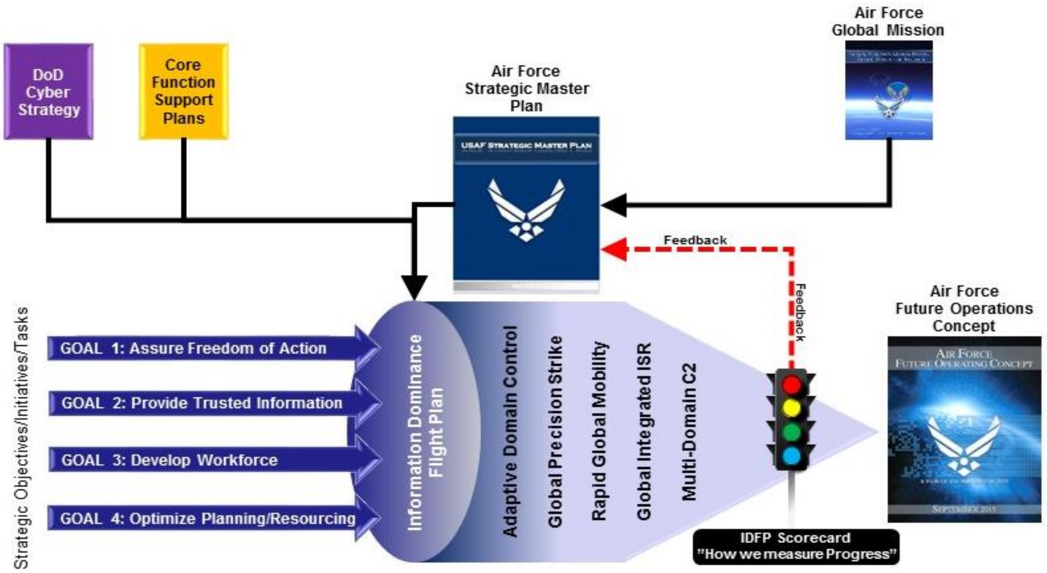


Figure-1: Air Force Strategic Master Plan (SMP) Alignment

The IDFP Strategic Framework (Figure-2), and Ops Approach (Figure-3) illustrate collaborative efforts required across the functional communities to achieve and maintain a unified, operational advantage for the Air Force core missions in, thru, and from cyberspace.



DoD Cyber Strategy
Core Function Support Plans
Air Force Strategic Master Plan
USAF STRATEGIC MASTER PLAN
Air Force Global Mission
Feedback
Feedback
Air Force Future Operations Concept
AIR FORCE FUTURE OPERATING CONCEPT
Strategic Objectives/Initiatives/Tasks
GOAL 1: Assure Freedom of Action
GOAL 2: Provide Trusted Information
GOAL 3: Develop Workforce
GOAL 4: Optimize Planning/Resourcing
Information Dominance Flight Plan
Adaptive Domain Control
Global Precision Strike
Rapid Global Mobility
Global Integrated ISR
Multi-Domain C2
IDFP Scorecard
"How we measure Progress"

Figure-2: IDFP Strategic Framework

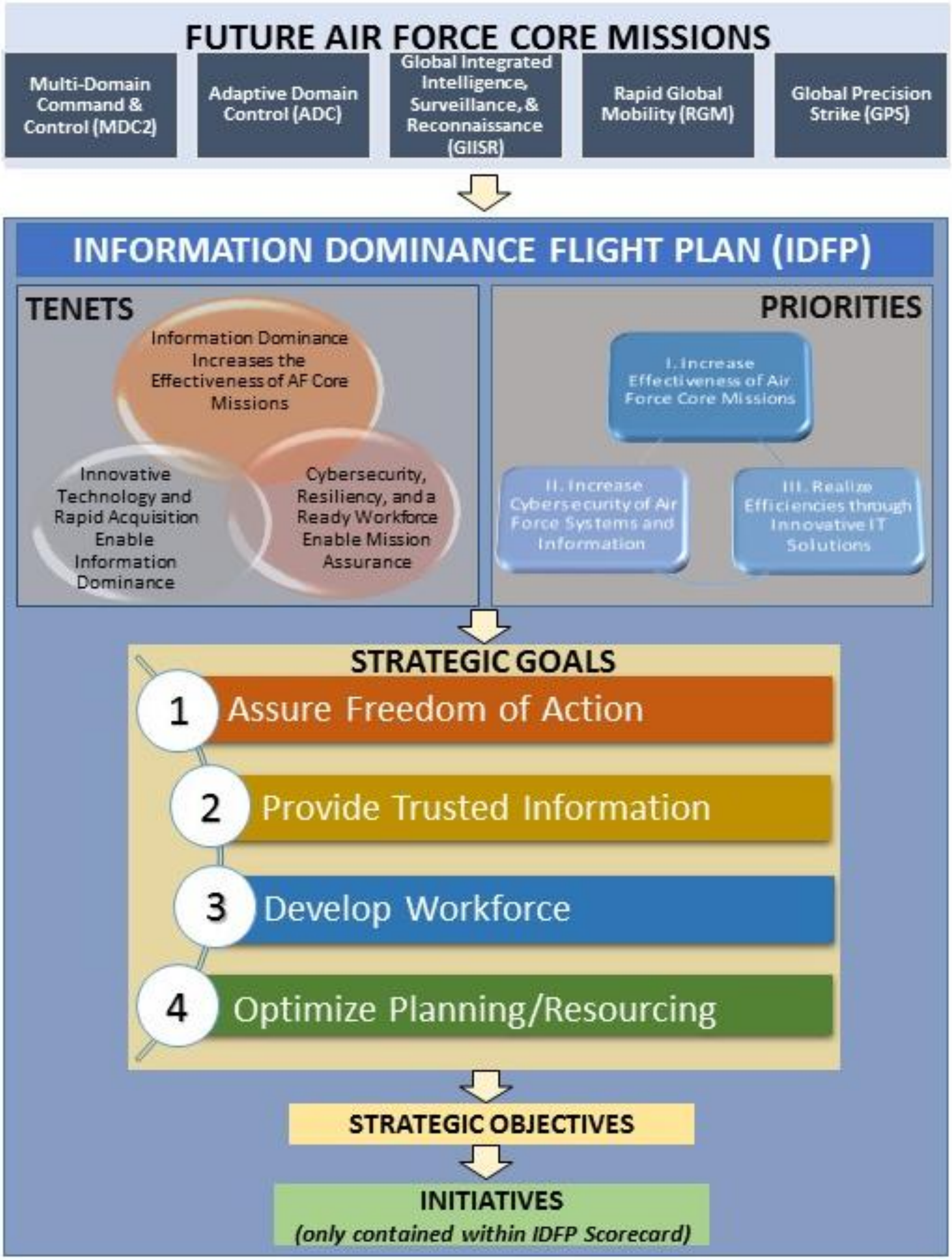

FUTURE AIR FORCE CORE MISSIONS
Multi-Domain Command & Control (MDC2)
Adaptive Domain Control (ADC)
Global Integrated Intelligence, Surveillance, & Reconnaissance (GIISR)
Rapid Global Mobility (RGM)
Global Precision Strike (GPS)
INFORMATION DOMINANCE FLIGHT PLAN (IDFP)
TENETS
Information Dominance Increases the Effectiveness of AF Core Missions
Innovative Technology and Rapid Acquisition Enable Information Dominance
Cybersecurity, Resiliency, and a Ready Workforce Enable Mission Assurance
PRIORITIES
I. Increase Effectiveness of Air Force Core Missions
II. Increase Cybersecurity of Air Force Systems and Information
III. Realize Efficiencies through Innovative IT Solutions
STRATEGIC GOALS
1 Assure Freedom of Action
2 Provide Trusted Information
3 Develop Workforce
4 Optimize Planning/Resourcing
STRATEGIC OBJECTIVES
INITIATIVES
(only contained within IDFP Scorecard)

Figure-3: IDFP Ops Approach

INFORMATION DOMINANCE, VISION, TENETS, AND PRIORITIES

Information Dominance Vision

Delivering Air Force cyber-power starts with understanding the Air Force **Vision for Information Dominance**: ***The Air Force fully exploits the man-made domain of cyberspace to execute, enhance, and support Air Force core missions.***

Airmen at every level need timely and accurate information to make decisions and act upon them.[7] Our ways of accessing and sharing information have evolved through innovation and technology. However, the pivotal role information has played in every campaign in the Air Forces' proud history has remained unchanged. Every Air Force mission depends upon **Information Dominance**: ***The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects.***

The IDFP's primary audience includes the Headquarters Air Force (HAF), the Air Force Major Commands (MAJCOMs), Lead-Commands, the Core Function Leads (CFLs), Program Executive Offices (PEOs) and any critical stakeholders responsible for acquisitions, planning, programming, and budgeting for future Air Force cyberspace initiatives. It also informs DoD, other federal agencies, coalitions and industry partners about the future direction of Air Force cyberspace. Through the lens of an *Information Dominance Vision*, collaboration across the Air Force and its mission partners will prepare the Air Force to Fly, Fight, and Win in Air, Space, and Cyberspace.

Information Dominance Tenets

Information Dominance is guided by three fundamental beliefs known as the Information Dominance tenets. The Information Dominance priorities below guide Air Force efforts in the pursuit of the interconnected tenets.

- ***Information Dominance Increases Effectiveness of Air Force Core Missions*****:** Information that is secure, accurate, reliable, and timely enables Information Dominance to warfighters by enabling the decision-cycle of observe, orient, decide, and act to outpace that of an adversary.
- ***Cybersecurity, Resiliency, and a Ready Workforce Enable Mission Assurance*****:** From concept design through full operational capability, the Air Force must integrate cybersecurity and resiliency throughout the lifecycle of weapon systems' in order to achieve mission assurance across all core missions. Airmen must practice responsible cybersecurity across the warfighting domains while maintaining the ability to fight through conflicts in contested cyberspace in order to achieve mission assurance.
- ***Innovative Technology and Rapid Acquisition Enable Information Dominance*****:** Innovation alone will not enable information dominance. Rapid and agile acquisition is critical to ensuring information technology and operational technology can respond to

[7] 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)

dynamic cyberspace requirements. Best practices from industry and mission partners should quickly be integrated into the Air Force cyberspace enterprise.

Information Dominance Priorities

In order to fulfill the USAF Strategic Master Plan's directive to identify "priority areas for investment, institutional change, and operational concepts,"[8] the IDFP identifies three priorities of effort:

1. **Increase Effectiveness of Air Force Core Missions**

   Maximum effectiveness is achieved when information is timely, accurate, relevant, and complete, ensuring that Airmen at every level can make informed decisions at superior decision speed. Information that arrives late or is full of errors is useless at best and an obstacle at worst. ***The Air Force will pursue solutions that prioritize the timeliness and accuracy of information.***

2. **Increase Cybersecurity of Air Force Systems and Information**

   Cybersecurity is crucial to the execution of Air Force core missions. The persistent and evolving cyberspace threat to the Air Force requires a holistic approach to cybersecurity that encompasses our people, culture, and operational processes. ***The Air Force will integrate cybersecurity throughout weapons systems development, testing, fielding, and employment. A culture shift in cybersecurity from compliance to resilience and risk mitigation across the Air Force will focus efforts on securing information across all of our core missions.***

3. **Realize Efficiencies through Innovative IT Solutions**

   As a man-made domain, cyberspace is fertile ground for innovation. We will tap the innovative ideas of Airmen, Industry, and Mission Partners to shorten the kill chain, increase the speed and quality of decision-making, and realize cost savings to enhance Air Force core missions. ***The Air Force will identify, vet, fund, implement, and sustain cyberspace initiatives that increase Air Force competitive advantages in its core missions.***

[8] The five strategic vectors are identified within the Air Force Strategic Master Plan: Provide effective 21st century deterrence; Maintain a robust and flexible ISR capability; Ensure a full-spectrum, high-end focused force; Pursue a multi-domain approach to our five core missions; and continue the pursuit of game-changing technologies. AF Strategic Master Plan, pg. 3, May 2015.

INFORMATION DOMINANCE FLIGHT PLAN GOALS

Information Dominance Flight Plan goals and objectives converge operational imperatives required to execute missions in air, space, and cyberspace. The principal focus is on information technology (IT), operational technology (OT), and cyberspace capabilities necessary to ensure successful execution of the Air Force core missions described in the AFFOC,[9] while denying adversary efforts to achieve information dominance over U.S. friendly and coalition forces, and vital national interests.

Air Force Core Missions of the Future

The Air Force portrays how it will conduct operations in the future as part of a joint, interagency, or multinational force, or independently in support of national security objectives through these five core missions.

Multi-Domain Command and Control (MDC2):

C2 of air, space, and cyberspace requires an "ability to plan, conduct, and assess *integrated multi-domain operations*."[10] This IDFP is focused on delivering the AFFOC's 2035 vision of a multi-domain C2 capability organized around the multi-domain operations center (MDOC). Agile delivery of IT/OT, optimized cyberspace investments, and the right mix of a cyber mission workforce will enhance the ability to deliver trusted information at a superior decision speed to Airmen and Joint Force Commanders. This timely information will allow U.S., joint, and allied forces to fully integrate global and regional assets necessary to ensure the flexibility and speed required to execute Air Force core missions and counter threats posed by potential adversaries.

Adaptive Domain Control (ADC):

In order to fly, fight and win in air, space, and cyberspace, the Air Force will pursue domain superiority to provide a "degree of dominance that permits the conduct of friendly operations at a given time and place."[11] Offensive and defensive cyberspace operations contribute to achieving and maintaining superiority by holding air, space, and cyberspace targets of interest at risk, while denying an adversary's pursuit of the same advantage. *Freedom of maneuver* and *domain superiority* require a degree of dominance that permits friendly operations at a time of our choosing while denying an adversary the same.

Global Integrated Intelligence, Surveillance, and Reconnaissance (GIISR):

Globally integrated ISR information systems are required for air, space, and cyberspace operations to collect, produce, exploit, disseminate and integrate disparate data and information to enable "leaders to make informed decisions at *superior decision speed*."[12] Advancements in data standards, security, interoperability, and architectural design, must be used to further automate access, integration and fusion of varying data and intelligence sources. This enables analysts to confidently predict adversary action. It also enhances the flexibility, commonality, and interoperability of C2 and communications providing integrated air, space, and cyberspace

[9] AFPD 17-1 defines IT as Any equipment, or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The Gartner IT Glossary defines operational technology (OT) as "hardware and software that detects or causes a change though the direct monitoring and/or control of physical devices, processes and events in the enterprise." Operational technology (OT) is further defined in Appendix1 – Terms.

[10] AFFOC., pg. 14

[11] AFFOC., pg. 18

[12] AFFOC., pg. 23

effects to the Joint Force Commander. GIISR operations demand near real-time flow of information over a global network unhindered by classification constraints and other barriers to the sharing of information with Joint, Allied, and Coalition partners. Through real-time collaboration, ISR will continue to be a vital source of information directly supporting our Nation's senior leaders' and warfighters' planning and decision making.

Rapid Global Mobility (RGM):

Projecting power across the globe by delivering the right effects, at the right place, and the right time requires harnessing "the power of total asset visibility and fully integrated information systems with predictive analysis to provide *superior decision speed* for users, planners, and operators."[13] RGM missions require cybersecurity across the "balanced capabilities mix of manned, remotely operated, and autonomous assets in both contested and uncontested environments."[14] The Air Force IDFP will inform resourcing decisions that enable the end-to-end mission set for RGM, with a focus on assuring the Air Force's ability to "deliver on demand."

Global Precision Strike (GPS):

The Air Force's ability to strike targets—anywhere and anytime—is a key component of our Nation's deterrence capability. Cyberspace operators will provide and defend weapon systems that enable the Air Force to hold adversary targets at risk. In addition, OCO offer unique alternatives to project power and increase Global Strike capabilities. Against a backdrop of increasingly contested global air, space, and cyberspace environments, OCO adds additional options for the Joint Force Commander to strike global targets. In order to maximize operational agility, the Air Force will ensure OCO capabilities are seamlessly integrated into global precision strike operations via a wide array of Air Force platforms.

Information Dominance Goals

Four *Information Dominance* goals will guide efforts within this flight plan toward achieving Air Force core missions. The first goal is the *main effort* for all Information Dominance activities across the Air Force, with three additional *supporting efforts*:

Goal 1: Assure freedom of action and deliver combat effects in, thru, and from cyberspace to advance the Air Force core missions.

The Air Force must have freedom of action in cyberspace to meet operational objectives in all domains. Freedom of action mitigates bad actors' attempts to interfere with operations and allows the Air Force to deliver combat power by exploiting cyberspace's unique characteristics.

This will be done through mission assurance, cyber force application and effective data-management. Airmen will proactively counter cyber-attacks, conduct ISR, and deliver effects in, thru, and from cyberspace to achieve multi-domain superiority. Additionally, cyberspace airmen will assess and manage cyber risk at acceptable levels to assure freedom of action across all domains. To realize this goal, organic Air Force cyber forces will be fully integrated across the Air Force core missions, while maintaining the ability to present mission ready forces to the nation's Cyber Mission Force.

[13] AFFOC, pg. 26
[14] AFFOC, pg. 26

Goal 2: Provide Airmen trusted information when and where they need it.

Airmen at all levels need timely, accurate, relevant, and complete information delivered in a way that ensures its availability, integrity, authentication, confidentiality, and nonrepudiation in order to make informed decisions. A trusted environment is critical for assuring this information across the full spectrum of air, space, and cyberspace operations. Mission assurance and the demand for information integrity require resiliency in an information environment with built-in security. Information-centric decision making requires an organization that delivers cross enterprise governance, and enforces data annotation, standards and retention across all security classification boundaries. The Air Force will achieve data stewardship by treating data as a critical asset and managing it accordingly.

The Air Force will invest in cyberspace capabilities that compress the information flow within the kill chain and apply common data standards in all mission areas with a focus on timeliness, accuracy, relevance, and completeness. System architectures of the future will seamlessly ingest data from various sources to provide the warfighter full spectrum situational awareness and the ability to outpace an adversary's capacity to observe, orient, decide, and act. Leveraging an Air Force enterprise architecture approach, Air Force core missions will benefit from greater operational and technical resilience, improved interoperability and effectiveness, enhanced integration across information systems, faster capability delivery, prioritized secure capabilities, and reduced costs.

Goal 3: Organize the cyber workforce, and train and educate all airmen to utilize the cyberspace domain to accomplish the Air Force missions.

Warfighter dependencies upon cyberspace require the Air Force to organize the cyber workforce, and train and educate all Airmen on cyberspace. Today's cyberspace vulnerabilities and risks span every domain and mission area. To counter potential threats, the Air Force must undergo a cultural shift from Industrial Age to Information Age thinking and acting in order to achieve Information Dominance. One such shift includes treating data as an asset, or more aptly a weapon system, and elevating our thinking and actions surrounding data management, control, and delivery beyond simply a support function to every core mission. Fostering innovation, improving policies, delivering agile and resilient organizations, and strengthen workforce agility will deliver these future Air Force needs. Employing new skills such as data science, as well as expanding existing data analytic capabilities is required to enable multi-domain information-centric decision making in an era of information warfare.

Training and education are required of all Airmen, not just cyber Airmen, so everyone understands the inherent risks cyberspace poses and how actions intended as harmless can impact cybersecurity. These efforts promote a Total Force workforce of skilled and qualified Regular Air Force (RegAF), Air Reserve Component and civilian Airmen prepared to support Air Force core missions.

To accomplish operational freedom of maneuver, the Air Force will recruit, retain and develop a more integrated cyber workforce. As the demand for cybersecurity, cyberspace operations, data-management, and enterprise architecture talent increases, the Air Force must improve its recruitment tactics to attract educated professionals into its workforce. Cyber forces will have foundational training and understanding of warfighter capabilities, operations planning, and commanders' priorities across all the combatant commands to meet Joint Force Commander (JFC) needs during wartime.

Airmen, through partnerships with industry, will continue to receive specialized training to ensure they are proficient within the role, system, and/or platform to which they are assigned. This will include continuous training and education throughout their careers to develop advanced skills.

The integration of cross-functional Airmen and capabilities are critical drivers of the fundamental concepts underlying joint and combined warfare. Integrating these functions enables joint and combined operations by providing relevant battlefield effects to combatant commanders. We will rapidly advance Air Force training programs to achieve Joint Training Certification, expeditiously incorporate lessons learned from the field into training curriculum, and deliberately manage the assignment process to develop Airmen as technical professionals and Air Force leaders.

The Air Force must also address the predicted worldwide shortage of cyber professionals that will impact the overall effectiveness of our cyber capabilities. We must develop effective strategies that create financial and non-financial incentives, enhance our cyber workforce skills, and emphasize meaningful development plans that incentivize Airmen and have an overall positive impact on retention.

Goal 4: Optimize the planning, resourcing, and acquisition requirements of cyberspace investments.

The Air Force will be at the forefront of driving and leveraging innovation in cyberspace in collaboration with the private sector and mission partners. The Air Force must rapidly identify, vet, fund, and implement innovative ideas that meet Air Force operational needs and enable operational innovation at the tactical edge.

Investment in cyberspace capabilities across the core functions must be transparent and aligned to SP3. The Air Force will manage its information technology and cyberspace capabilities portfolios to ensure the competitive advantages available from information technology and national security systems investments are realized. The Air Force will maximize its cyberspace investments by leveraging commercial support and services that directly enhance core missions.

To achieve this goal, we will develop and institute an agile and strong governance structure and processes to rapidly identify and procure mission requirements with requisite mission partners. We will pursue a unified information technology portfolio to manage cyber/IT investments via a formalized investment review processes that informs governance, the AF corporate process, and the SP3. Additionally, we will seek new and agile capabilities through coordination with industry and mission partners to co-share and drive-down research and development costs where mutually beneficial in delivering secure and resilient technologies. Air Force policies and procedures will change to enable new financial and IT performance controls and support automated IT asset management that improves accountability and compliance. Finally, we will establish an enterprise architecture process to drive planning and investment decision-making that ensure interoperability, reduce risk and duplication of procurement efforts, and align resources toward mission assurance.

IDFP OBJECTIVES

Executing the IDFP requires a plan for execution, accountability, and guiding progress. Initial *objectives* help guide plans for execution and provide a starting point for Offices of Primary Responsibility (OPRs) to develop *initiatives* necessary for goal achievements.

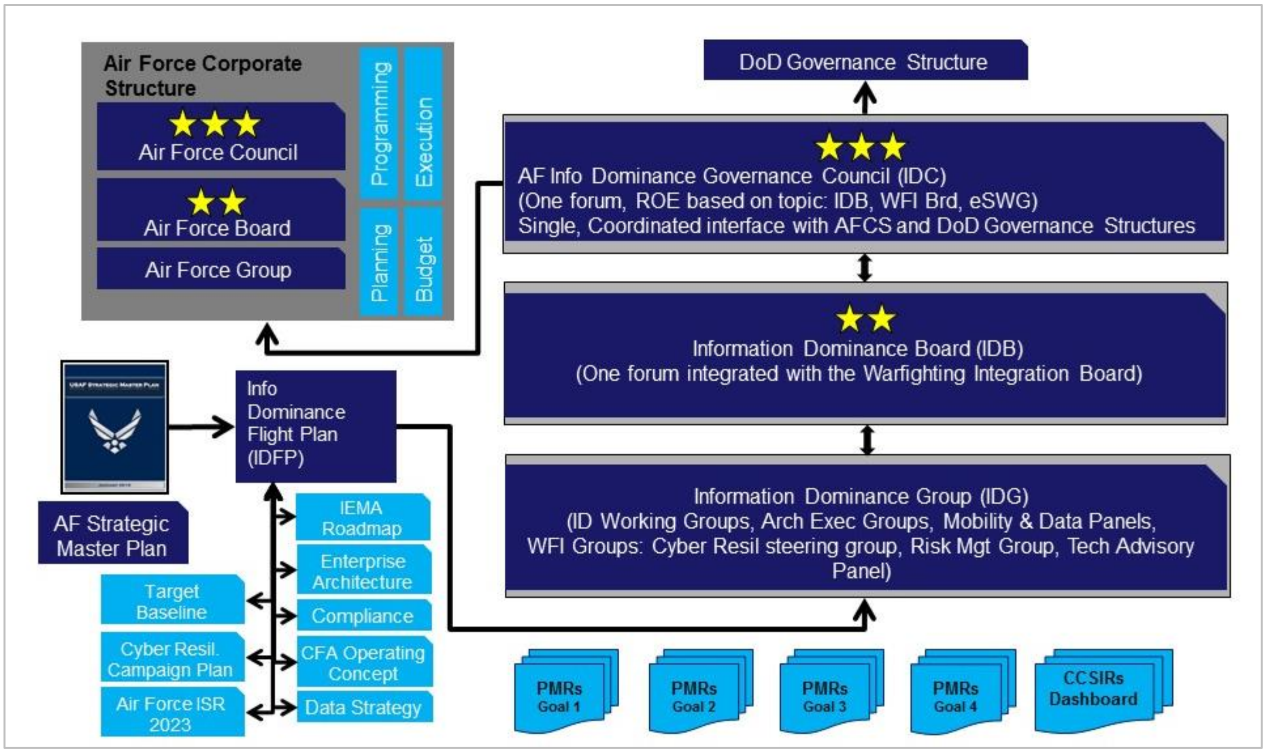
Annex 2 lists each of the initial objectives organized by the strategic goals. It describes each goal with a statement of a challenge, a vector toward the desired end state, and a description of the actions to be taken. It also links the objective to the SMP and assigns an OPR. It is presumed that Information Dominance objectives will change over time and that these changes will be incorporated into an amended IDFP annex as required.

GOVERNANCE / MEASURING SUCCESS

To track progress of the IDFP, the Air Force will perform three activities: (1) use a scorecard approach to measure objectives and initiatives developed by each OPR; (2) conduct periodic Performance Metric Reviews (PMRs) to provide an internal Air Staff deep-dive of initiatives in direct support of a defined objective; and; (3) leverage the Air Force governance framework (Figure-4) utilizing the Information Dominance Board and Information Dominance Council for investment and operational priorities decision making by Air Force leaders.

Governance

Effective governance is critical to the successful application and achievement of the IDFP's goals. The operational cyberspace imperatives of the Air Force functional communities will be met through prioritization of effort and resources necessary to achieve IDFP goals. To be effective, the governance structure must reflect the breadth of activities and organizations responsible for achieving the SP3 responsibilities of this Flight Plan.



Air Force Corporate Structure
★★★
Air Force Council
★★
Air Force Board
Air Force Group
Programming
Execution
Planning
Budget
DoD Governance Structure
★★★
AF Info Dominance Governance Council (IDC)
(One forum, ROE based on topic: IDB, WFI Brd, eSWG)
Single, Coordinated interface with AFCS and DoD Governance Structures
★★
Information Dominance Board (IDB)
(One forum integrated with the Warfighting Integration Board)
Information Dominance Group (IDG)
(ID Working Groups, Arch Exec Groups, Mobility & Data Panels, WFI Groups: Cyber Resil steering group, Risk Mgt Group, Tech Advisory Panel)
USAF STRATEGIC MASTER PLAN
AF Strategic Master Plan
Info Dominance Flight Plan (IDFP)
IEMA Roadmap
Enterprise Architecture
Compliance
CFA Operating Concept
Data Strategy
Target Baseline
Cyber Resil. Campaign Plan
Air Force ISR 2023
PMRs Goal 1
PMRs Goal 2
PMRs Goal 3
PMRs Goal 4
CCSIRs Dashboard

Figure 4: Information Dominance Governance Framework

In concert with the IDFP, a strategic management scorecard system will track progress and escalate matters to and through the Information Dominance governance structure. All four IDFP Goals will be reviewed at least quarterly at the Information Dominance Council. Goal 1 will be reviewed through the Warfighting Integration Board (WFI Board), which will cover freedom of action in, thru, and from cyberspace. Goals 2, 3, and 4 will be reviewed through the Information Dominance Board, which will focus on trusted information, workforce development as well as planning and resourcing matters. Given the collaborative nature of the IDFP support to the Air

Force cyberspace enterprise, it is envisioned that any functional community from across the Air Force with a warfighting requirement dependent upon cyberspace will employ the Information Dominance governance structure. This reporting process and governance structure aligns with AF/A5/8's process for assessing progress toward the Air Force Strategy and SMP goals and objectives.

Scorecard

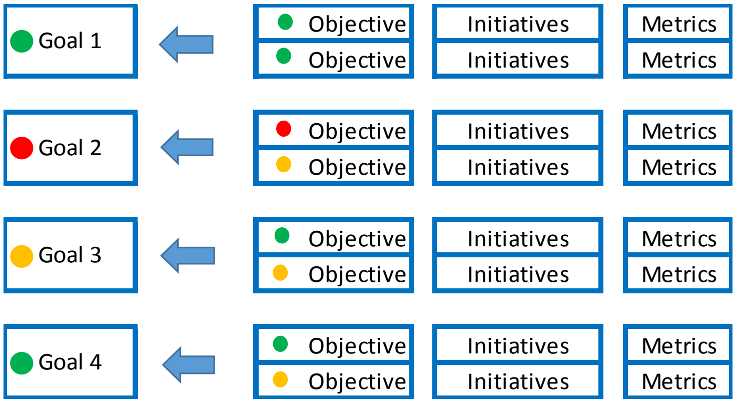


Figure 5: IDFP Scorecard

The IDFP Scorecard is a collaborative strategy management system that enables the Air Force to ensure effort is focused on making progress toward its stated goals and objectives. It is the framework for managing the IDFP implementation of strategy while allowing the strategy to evolve in response to changes in the political, operational and technological environments. IDFP goal achievement will be managed through a scorecard approach employed to evaluate success and rapidly identify when goals and objectives encounter resistance to successful execution. The building blocks of the scorecard are the individual initiatives; discrete, measurable activities designed to contribute to the accomplishment of one or more objectives. Initiatives are aligned to the respective objectives and weighted according their assessed value to that objective. The weighting and assessment responsibilities belong to the OPR with oversight by the Information Dominance governance processes and procedures. Goals, Objectives and Initiatives are reviewed by their respective OPRs on a regular basis in order to establish a reliable overview of IDFP progress and focus. Based on defined metrics, the status of each element is assessed as red/amber/green or blue, with the latter denoting complete (Figure 5). Detailed guidance on the IDFP Scorecard is incorporated into the Scorecard on SharePoint.

Performance Metric Review (PMR)

The purpose of the PMR is to have an internal organizational discussion with the responsible senior leaders to determine the gaps, risks, priorities, costs, and opportunities that lie ahead in order to meet IDFP goals. To report progress of the IDFP, periodic PMRs will be conducted using the IDFP Scorecard metrics developed for each objective and initiative. Reporting performance using these metrics will improve communication and collaboration across the staff, as well as coordinate actions, provide strategic direction, and drive support to operations.

Through this system, the impact of initiatives on strategic performance can be measured, providing a data-driven foundation for analyzing the success toward strategic objectives and goals. This type of analytics provides value-based decision making through persistent risk analysis.

SUMMARY

The purpose of the IDFP is to organize cyberspace initiatives over the next 10-years across the Air Force. Unified and consolidated actions are critical to ensure unity of action toward fully exploiting cyberspace. Strong top-down leadership is necessary to inspire new ideas and innovative behaviors in our workforce. The IDFP seeks to enable Air Force core missions by assuring freedom of maneuver in, thru, and from cyberspace.

The future Air Force cyber operations organizational structure must focus on mission assurance and a ready workforce. The Air Force must expand its focus beyond maintaining the Air Force enterprise network and move toward building, operating, securing, defending, extending, exploiting and engaging in cyberspace while protecting Air Force weapon and mission systems in a contested cyberspace environment. Air Force cyber and data-management capabilities must evolve to produce competitive multi-domain advantages against potential adversaries. Achieving these desired future-states starts with a ready workforce engrained in a culture of risk assessment and risk mitigation required to execute the Air Force core missions.

From permissive to highly contested environments, information dominance must enable the full spectrum of cyberspace operations at the time and place of our choosing, while denying the same to an adversary. Airmen will continue to enable joint warfare by integrating the full spectrum of cyberspace operations with an in-depth understanding of the missions in, thru, and from cyberspace. Multi-domain operations require robust integration across air, space, and cyberspace for the greater purpose of achieving our Air Force and joint force objectives. This flight plan, in concert with Air Force strategic guidance, is a necessary strategic planning component in support of national security.

ANNEX 1 – LINKING IDFP GOALS TO THE STRAGIC MASTER PLAN (SMP)

The Strategic Master Plan (SMP) translates the Air Force's 30-year strategy, *America's Air Force: A Call to the Future*, into a 20-year plan consisting of comprehensive goals and objectives.[15] The following section links the IDFP's 10-year goals to the SMP.

GOAL 1: Assure freedom of action and deliver combat effects in, thru and from cyberspace to advance the Air Force core missions.

- **AG1.4** Combine training across multiple mission sets, including integrated live, virtual and constructive (LVC) venues and operator-in-the-loop Modeling & Simulation (M&S), to cultivate Airmen trained in agile and robust decision-making who can devise multi-domain solutions to complex problems in uncertain, contested environments.
- **AG2.1** Ensure systems are designed, engineered, tested, acquired, and sustained smartly, efficiently, and cost-effectively. As integrator, the Air Force will define technical baselines and common architectures and ensure modularity and responsiveness to Airmen's needs in a dynamic strategic environment.
- **AG2.3** Develop an "agile acquisition" mindset that challenges bureaucratic inertia, streamlines processes, implements continuous improvement, and reduces risk through prototyping and new engineering development models.
- **AG3.1** Foster Air Force organizations that responsibly learn from minor setbacks in pursuit of major achievements.
- **AG3.3** Educate, train, and empower Airmen to implement agile, tailored approaches to organization and accountability, to modify counterproductive practices, and to improve lateral and vertical collaboration.
- **DTR.2** Develop, test, and implement additional non-nuclear capabilities that deter a wide range of adversaries, including non-state actors, and assure allies and partners. Consider low-cost measures that generate high-cost adversary responses.
- **FH1.1** Ensure the ability to gain and maintain the required degree of control of the air to prevent effective enemy interference with friendly operations.
- **FH1.2** Ensure viable options are available to sustain capabilities provided by space assets in case they are challenged or denied, particularly for position, navigation, timing, strategic warning and communications. This includes both resilient space systems and non-space systems.
- **FH1.3** Strengthen capabilities that enable freedom of action in cyberspace and enhance

[15] Air Force Strategic Master Plan, May 2015, p 3

our ability to deny the same to adversaries

- **FH1.4** Enhance abilities to degrade or deny situational awareness and targeting ability to an advanced enemy.
- **FH1.5** Reduce emphasis on tactical tasks in permissive environments where other Services have sufficient organic capacity (for example tactical ISR, fire support and intra-theater mobility).
- **FH2.2** Increase emphasis on stand-off capabilities that maximize speed, range and flexibility, while maintaining the ability to transition to effective resilient presence in the battlespace.
- **FH2.4** Improve flexibility, commonality, and interoperability of our C2 and communications to integrate air, space, and cyberspace effect delivered by different Services or agencies.
- **FH2.7** Provide resilient installations, infrastructure and combat support capabilities that enable the Air Force to rapidly project power effectively and efficiently.
- **MDA.1** Orient the Air Force to a mindset that intuitively considers multi-domain options when solving complex problems, to include development of doctrine and tactics, techniques, and procedures (TTPs).
- **MDA.2** Reappraise existing compartmentalization practices and eliminate institutional barriers to empower Airmen and organizations to employ multi-domain approaches.
- **ISR.1** Rebalance resilient ISR sensors, systems, and processes toward operations in high-end contested environments, and focus on moderately priced systems, to include commercial technology, for permissive environments.
- **ISR.2** Develop a robust, survivable, secure architecture to connect and integrate ISR operations across all domains, ensuring that collection and analytic systems (including non-traditional ISR platforms and sensors) and users can collaborate seamlessly.
- **ISR.3** Increase flexibility and standardization in ISR processes and knowledge management tools to minimize delays and regulatory obstacles, enabling analysts to provide rapid, decision-level intelligence to overcome adaptive adversaries.
- **ISR.4** Enhance capabilities to holistically detect, monitor, analyze, and attribute threats (kinetic or non-kinetic), adversaries, and their support networks, and improve target systems analysis to determine the best way to act on this intelligence.
- **ISR.5** Improve policies, processes, and organizations for obtaining, sharing, and releasing pertinent multi-domain intelligence with joint, interagency, and international partners.

GOAL 2: Provide airmen trusted information when and where they need it.

- **AG2.1** Ensure systems are designed, engineered, tested, acquired, and sustained smartly, efficiently, and cost-effectively. As integrator, the Air Force will define technical baselines and common architectures and ensure modularity and responsiveness to Airmen's needs in a dynamic strategic environment.
- **FH1.1** Ensure the ability to gain and maintain the required degree of control of the air to prevent effective enemy interference with friendly operations.
- **FH1.2** Ensure viable options are available to sustain capabilities provided by space assets in case they are challenged or denied, particularly for position, navigation, timing, strategic warning, and communications. This includes both resilient space systems and non-space options.
- **FH1.3** Strengthen capabilities that enable freedom of action in cyberspace, and enhance our ability to deny the same to adversaries.
- **FH2.2** Increase emphasis on stand-off capabilities that maximize speed, range, and flexibility, while maintaining the ability to transition to effective, resilient presence in the battlespace.
- **FH2.4** Improve flexibility, commonality, and interoperability of our C2 and communications to integrate air, space, and cyberspace effects delivered by different Services or agencies.
- **FH2.6** Improve execution speed and situational understanding through advances in human-machine teaming, automated processing, exploitation and dissemination (PED), analysis, and updated C2 and communication capabilities.
- **FH2.7** Provide resilient installations, infrastructure, and combat support capabilities that enable the Air Force to project power rapidly, effectively, and efficiently.
- **IN3.3** Deepen our relationships with the joint team, intelligence community, diplomatic institutions, developmental agencies, local governments, businesses, communities, and international partners through sustained dialogue, increased training and exchange, aviation security cooperation, and iterative enterprises to codify shared doctrine, tactics, and capabilities.
- **ISR.1** Rebalance resilient ISR sensors, systems, and processes toward operations in high-end contested environments, and focus on moderately priced systems, to include commercial technology, for permissive environments.
- **ISR.2** Develop a robust, survivable, secure architecture to connect and integrate ISR operations across all domains, ensuring that collection and analytic systems (including non-traditional ISR platforms and sensors) and users can collaborate seamlessly.
- **ISR.3** Increase flexibility and standardization in ISR processes and knowledge management tools to minimize delays and regulatory obstacles, enabling analysts to

provide rapid, decision-level intelligence to overcome adaptive adversaries.

- **ISR.4** Enhance capabilities to holistically detect, monitor, analyze, and attribute threats (kinetic or non-kinetic), adversaries, and their support networks, and improve target systems analysis to determine the best way to act on this intelligence.
- **ISR.5** Improve policies, processes, and organizations for obtaining, sharing, and releasing pertinent multi-domain intelligence with joint, interagency, and international partners.

GOAL 3: Organize the cyber workforce, and train and educate all airmen to utilize the cyberspace domain to accomplish the Air Force missions.

- **AG1.1** Recruit/assess individuals with demonstrated potential for critical thinking, adaptive behavior, character, initiative, innovation, and contemporary mission-critical skills.
- **AG1.2** Implement an individually tailored, generationally appropriate, cutting-edge, life-long approach to education and training.
- **AG1.3** Ensure institutional processes and culture value individual initiative, support productive failure in pursuit of innovation, provide latitude to experiment, and instill a cost-conscious mindset in all Airmen.
- **AG1.4** Combine training across multiple mission sets, including integrated LVC venues and operator-in-the-loop M&S, to cultivate Airmen trained in agile and robust decision-making who can devise multi-domain solutions to complex problems in uncertain, contested environments.
- **AG1.5** Preserve full-spectrum warfighting, expeditionary, and combat support capabilities by retaining expert Airmen with experience in recent conflicts, codifying lessons learned, and further integrating joint training (including LVC) to offset reduced resourcing for low-intensity operations.
- **AG1.6** Modernize Airman management mechanisms to ensure they value and provide increased opportunities for broad and varied professional experience; enable the continuum of service; improve Commander- and Airman-level professional development; and provide career-long, proactive retention measures beyond financial incentives.
- **AG3.2** Rigorously reevaluate and adjust Air Force organizational structures to address a dynamic security environment.
- **AG3.3** Educate, train, and empower Airmen to implement agile, tailored approaches to organization and accountability, to modify counterproductive practices, and to improve lateral and vertical collaboration.
- **GCT.1** Increase the technical acumen of all Airmen to enable greater innovation and experimentation.

- **IN1.1** Produce decision makers adept in finding creative ways to access the force structure and optimizing it to meet mission demands. Focus on arming a generation of leaders with doctrine, history, and experience to provide cross-component expertise
- **IN1.2** Incorporate Total Force considerations wherever possible to increase the flexibility of our force structure and optimize our operational responses. Focus on identifying appropriate force mix options, eliminating structural and legal barriers, and increasing opportunities for component integration.
- **IN2.3** Orient and educate the force to the idea that a blend of varied perspectives, cognitive approaches, and critical thought is a vital combat capability and integrate it into all aspects of our operations. Focus on eliminating institutional barriers to creating and retaining a diverse team.
- **FH2.6** Improve execution speed and situational understanding through advances in human-machine teaming, automated PED, analysis, and updated C2 and communication capabilities.
- **ISR.5** Improve policies, processes, and organizations for obtaining, sharing, and releasing pertinent multi-domain intelligence with joint, interagency, and international partners.
- **ISR.6** Professionalize ISR analysis through training, tradecraft (including cultural competencies), and collaboration; restore analytic and targeting competencies.
- **MDA.1** Orient to a mindset that intuitively considers multi-domain options when solving complex problems, to include development of doctrine and TTPs.
- **MDA.2** Reappraise existing compartmentalization practices/eliminate institutional barriers to empower Airmen and organizations to employ multi-domain approaches.

GOAL 4: Optimize the planning, resourcing, and acquisition requirements of cyberspace investments.

- **AG2.1** Ensure systems are designed, engineered, tested, acquired, and sustained smartly, efficiently, and cost-effectively. As integrator, the Air Force will define technical baselines and common architectures and ensure modularity and responsiveness to Airmen's needs in a dynamic strategic environment.
- **AG2.2** Improve acquisition tradecraft and business acumen by actively managing people with the appropriate education, training, and skills; and increasing efficiency and effectiveness in acquisition tools and techniques (including disciplines like systems engineering and digital thread tools).
- **AG2.3** Develop an "agile acquisition" mindset that challenges bureaucratic inertia, streamlines processes, implements continuous improvement, and reduces risk through prototyping and new engineering development models.

- **AG2.4** Incentivize innovative solutions and improve competition in the defense industrial base by providing transparency and stability in requirements and funding, increasing competitive bids, reducing developmental risks, and encouraging partnering with industry.
- **AG2.5** Establish an agile capability development framework that leverages credible and defendable knowledge resulting from development planning and experimentation activities to inform the Sp3 decisions.
- **AG3.3** Educate, train, and empower Airmen to implement agile, tailored approaches to organization and accountability, to modify counterproductive practices, and to improve lateral and vertical collaboration.
- **FH2.1** Increase emphasis on research, development, testing, and evaluation (RDT&E) for capabilities that ensure the ability to find, fix, track, target, engage and assess effects against critical target sets in highly contested environments.
- **GCT.2** Provide senior leadership with timely S&T options, best matched to the security environment, that maintain or advance asymmetric advantages in air, space, and cyberspace and that inform and accelerate capability development through experimentation campaigns and developmental planning efforts.
- **IN1.3** Synchronize programming and planning across the Active and Reserve Components to enable specific and timely input to the HAF that ensures adequate time to align ARC planning and programming efforts.

ANNEX 2 – IDFP STRATEGIC OBJECTIVES

GOAL 1: *Assure freedom of action and deliver combat effects in, thru, and from cyberspace to advance the Air Force core missions.*

FREEDOM OF ACTION		
Objective 1.1 - Develop and integrate cyber capabilities to deliver combat effects to achieve the core missions. *(OFFENSE)*	**SMP Links**	**OPR**
Challenge: Commanders need effective, relevant, and responsive cyber warfare capabilities integrated into multi-domain operations to achieve the core missions. The Air Force simply cannot build standalone cyber capabilities and place them in virtual bunkers for wartime use without a reliable measure of effectiveness or plan for employment. Additionally, the Air Force cannot deliver combat effects in, thru, and from cyberspace against an adversary without leveraging the additional access and reach provided by the air and space domains. **Vector:** The Air Force requires an end-to-end, multi-domain capability to gain access to targeted adversary systems, enable the ability to hold targets at risk, and develop reliable cyberspace weapons for employment when authorized. **Action:** Develop cyber forces and capabilities requirements, (i.e. platform, payloads, and access) through the acquisition community in order to generate effects in all domains. This process will start with a strategy-to-task construct and link commanders' strategic and operational needs with tailored capability development. It will produce institutional forces who can conduct multi-domain ISR; advanced target development; access development; and capability development, integration, and deployment. This future-state will be accomplished using a continuous and iterative process to provide operationally agile options to commanders.	**AG1.4** **AG2.1** **DTR.2** **FH1.3** **FH1.4** **FH2.4** **MDA.1** **MDA.2** **ISR.1** **ISR.2** **ISR.3** **ISR.4**	**AF-A3C/A6C**
Objective 1.2 - Protect and assure the ability to accomplish Air Force missions. (*DEFENSE)*	**SMP Links**	**OPR**
Challenge: Nearly all Air Force's capabilities reside in or rely on cyberspace. In order to position the Air Force to accomplish the five core missions in a contested cyberspace environment, all commanders must understand the operational impact of cyber threats and be able to mitigate them. **Vector:** The Air Force will focus on embedding cyber-awareness into Air Force organizational culture. It will refine policies, clarify responsibilities, and enable resource sharing for mission assurance. Cyber Squadrons, focusing on mission assurance[16], will retain the	**AG1.4** **AG2.1** **AG2.3** **AG3.3** **DTR.1** **FH1.1** **FH1.2** **FH1.3** **FH1.5** **FH2.2**	**SAF/CIO-CISO**

[16] Sources: Air Force Cyberspace Operations Strategy 2015;In/Through/From Cyber Memo

responsibility to provide trusted information to warfighters. Assuring the mission in a contested environment requires not only robust cyber defenses, but also the ability to continue operations and respond to disruptions when cyber-attacks breach those defenses. **Action:** Optimize the organizational structure, responsibilities, and authorities to more effectively manage enterprise cybersecurity risk. The Air Force will integrate mission assurance into operations and planning processes. Wings will complete and maintain Functional Mission Analysis (FMA) leveraging both the Air Force Campaign Plan mission thread analysis results and current intelligence to identify key terrain in cyberspace. Cyberspace squadrons will conduct active defense of their wings' missions and appropriately inform commander risk decision-making.[17]	**FH2.4** **FH2.5** **MDA.1** **MDA.2** **ISR.1** **ISR.2** **ISR.3**	
Objective 1.3 - Increase cybersecurity and resiliency of Air Force weapon and mission systems, including IT, OT, and platform. *(WEAPON SYSTEMS)*	**SMP Links**	**OPR**
Challenge: In order to position the Air Force to accomplish the five core missions in a contested cyberspace environment, all commanders must understand the operational impact of cyber threats and be able to mitigate them. **Vector:** The Air Force must adopt an approach to mission assurance that identifies and defends key cyber terrain. Identifying cyber key terrain, including where it extends beyond traditional IT systems into critical operational technologies (OT) like logistics systems, weapon systems, and decision support systems, sensors, etc., allows commanders to focus cyber defense resources on areas of highest risk to the mission. **Action** The Air Force will employ a Cyber Campaign Plan's Mission Thread Analysis execution plan to identify and manage risk throughout the lifecycle of all Air Force IT, inclusive of information systems, platform IT, and operational technology (OT). The Air Force will apply Functional Mission Analysis (FMA) to identify systems where cybersecurity is paramount. Air Force defined network risk models and processes will ensure a managed and secure baseline for IT. Comprehensive damage assessments of cyber intrusions to defense contractor networks will document the compromise of DoD information external to DoD-operated networks.	**AG2.1** **DTR.2** **FH1.1** **FH1.3** **FH2.4** **FH2.7** **MDA.2**	**SAF/CIO-CISO** **SAF/AQ (OCR)**
Objective 1.4 - Characterize cyberspace threats and understand adversaries' capabilities. *(INTELLIGENCE)*	**SMP Links**	**OPR**
Challenge: Cyberspace is an environment in which we must understand the tactical and operational impact of cyber threats and	**ISR.1** **ISR.2**	**AF-A2C**

[17] Sources: Air Force Cyberspace Operations Strategy 2015;In/Through/From Cyber Memo

vulnerabilities. Given these risks, the Air Force must have capabilities to mitigate mission risk and continue critical operations even in a degraded cyberspace environment. Potential adversaries continue to acquire and develop relatively low-cost, asymmetric capabilities that threaten our access to, and freedom of action in cyberspace. **Vector:** Detecting and analyzing ongoing and persistent intrusions and use of our networks, while predicting adversary intentions and capabilities will require agile, resilient, and innovative ISR capabilities operating in all domains by a highly skilled workforce. Anticipating adversary actions in the cyber domain requires continuous analysis of adversary national strategy and kinetic and non-kinetic doctrine as they apply to USAF systems throughout all phases of military conflict. This analysis should develop detailed cyber threat models aligned with an intelligence-derived understanding of adversary effects. **Action:** Invest in ISR capabilities to collect, store, and analyze data traversing the AF Information Network (AFIN) [AFNET, Industrial Control Systems / Supervisory Control And Data Acquisition (ICS/SCADA), maintenance terminals, mission planning systems, avionics, aircraft, and space systems, etc.] to provide Indications & Warnings of immediate and developing cyberspace threats using integrated intelligence sources to provide real-time analysis. Additionally, incorporate automation and autonomy for the analysis of data collected in cyberspace. Advanced ISR analytic tools and capabilities in cyberspace are vital for data mining large amounts of data, automating repetitive processes, identifying anomalous behavior, contributing to situational awareness, and enabling the execution of pre-authorized actions. Teaming human analysis with automated systems is crucial for the cyberspace domain, where the speed and abundance of information makes human processing difficult to accomplish in the time required to support dynamic cyberspace operations.	**ISR.3** **ISR.4** **ISR.5** **MDA.1** **MDA.2**	
Objective 1.5 – Develop advanced cyberspace ISR capability requirements. *(EXPLOIT)*	**SMP Links**	**OPR**
Challenge: Cyberspace provides opportunities to collect intelligence information that may be unattainable through the other domains. This intelligence will be used to support operations in all domains and provide critical information to decision makers from the tactical to strategic level. **Vector:** ISR operations in cyberspace will leverage platforms operating in all domains to gain access to otherwise closed or isolated networks. **Action:** Develop and acquire advanced ISR capabilities integrated on air-, space-, and cyberspace-based platforms that provide access to	**FH1.3** **FH1.4** **FH2.6** **ISR.1** **ISR.2** **ISR.3** **ISR.4** **ISR.5** **MDA.1** **MDA.2**	**AF-A2C** **SAF/AQ (OCR)**

information in otherwise denied areas. Coordinate with SAF/AQ to deliver required capabilities.		
Objective 1.6 – Develop and employ an Air Force-wide cyberspace risk methodology. *(RISK)*	**SMP Links**	**OPR**
Challenge: The Air Force does not have a methodology to measure and assess cyberspace risk from an enterprise perspective. **Vector:** Decision makers must have a model to assess risk between Air Force core missions and the mission systems that enable those missions. **Action:** Develop and maintain a cyberspace risk methodology to measure risk across the cyberspace enterprise relative to mission systems and Air Force core missions. The Air Force must identify mission-critical cyber assets and assure they can operate in a contested environment. This objective will support the Air Force Cyber Campaign Plan mission thread analysis activity.	**AG2.1** **AG3.1** **AG3.3** **FH1.1** **FH1.3** **FH2.5** **MDA.2** **ISR.5**	**SAF/CIO-CISO**

GOAL 2: Provide airmen trusted information when and where they need it.

INFORMATION ACCESS		
Objective 2.1 –Optimize AF Information and Intelligence Networks. *(COMPUTE/STORE)*	**SMP Links**	**OPR**
Challenge: The Air Force Information Network (AFIN), ISR and other domains are characterized by duplicative capabilities plagued by vulnerabilities, incompatibilities, and excess costs. Air Force missions demand IT services to execute core missions. **Vector**: The Air Force must harness cloud computing, commodity and enterprise IT services, leverage DoD and IC capabilities to increase mission effectiveness and cybersecurity while reducing costs. **Action**: Evaluate, resource, and employ cloud services that enable mission assurance. Host limited Air Force specific applications when required to meet the needs of Air Force core missions. Avoid development of unique Air Force application solutions; employ industry/commercial solutions. Evaluate, resource, and employ software, platform, and infrastructure "as a service" solutions that focus on mission assurance and cyber security of Air Force core missions. Consolidate duplicative and interrelated systems into a single enterprise level capability. The Air Force will migrate from legacy technology where operationally relevant (i.e. Joint Information Environment adoption).	**AG2.1** **FH1.1** **FH1.3** **FH2.2** **FH2.4** **FH2.7** **ISR.1** **ISR.2** **ISR.3**	**SAF/CIO-A6S**

Objective 2.2 – Ensure robust connectivity, resiliency and flexibility across Air Force Information and Intelligence Systems. ***(CONNECT)***	**SMP Links**	**OPR**
Challenge: Cyberspace is vulnerable to adversarial action, natural events, and technological issues – any of which can threaten Air Force core missions. Mission assurance and information integrity require resilient connectivity. **Vector:** Air Force cyberspace must be resilient and self-healing to ensure availability in a contested, degraded, or operationally limited (CDO) environment. Partnership, collaboration and teamwork on scales previously unrealized will be required. **Action:** The Air Force will create an agile, federated enterprise that extends to the tactical edge supporting data and information availability. Ensure an enterprise that is able to operate in the contested and uncontested environments, to include bandwidth constrained. Research, identify, develop, and implement resilient and self-healing mission-critical Information and Intelligence networks.	**AG2.1** **FH1.2** **FH1.3** **FH2.4** **FH2.7** **ISR.2** **ISR.3** **ISR.4**	**SAF/CIO-A6S** **SAF/AQ (OCR)**
Objective 2.3 – Assure the availability, integrity and confidentiality of information in cyberspace. ***(PROTECT)***	**SMP Links**	**OPR**
Challenge: Airmen require accurate and secure information to execute Air Force core missions. **Vector:** Information in cyberspace must be protected commensurate with its classification and value to national security. The complexity of securing information that resides or passes through Air Force systems, including networks, weapon systems, and space systems, requires protection and mitigation from threats. **Action:** Air Force must work closely with NSA, OSD, Joint Staff, and industry partners developing aggressive courses of actions to meet cryptographic threats and to develop mitigating actions that ensure critical information and weapon systems remain secure and free to operate in cyber contested environments.	**AG2.1** **FH1.1** **FH1.3** **FH2.4** **IN3.3** **ISR.1** **ISR.2** **ISR.5**	**SAF/CIO-CISO**
Objective 2.4 – Provide secure mobile access to required information for mission efficacy. ***(END DEVICES)***	**SMP Links**	**OPR**
Challenge: Current policies, network infrastructure, and end-user devices limit the ability to fully exploit the potential of wireless technologies. This limits Airmen's ability to access real-time information from anywhere in the world and to rapidly acquire and integrate useful commercial and public applications, tools and data without the expense and manpower required to sustain a global wired infrastructure plant. Although there are a variety of wireless solutions implemented at Air Force installations across the world, these adoptions of mobile capability have, as a rule, been local (or at best	**FH2.2** **FH2.4** **FH2.6** **FH2.7** **ISR.2**	**SAF/CIO-A6S**

MAJCOM-wide) solutions, implemented on legacy systems riding on the legacy wired infrastructure. Because of interoperability and security concerns, few of these solutions have fully exploited the potential of wireless technologies. **Vector**: Advance the IT policies, processes, infrastructure, and end-user devices to support end-to-end wireless access and security, in which all information is accessible anywhere at any time by any authorized personnel. **Action**: The Air Force will improve the network to support mobile access to applications, data and tools. The Air Force will move towards a single security and management framework that is device agnostic. The Air Force will also address gaps in mobility guidance and policy.		
Objective 2.5 – Ensure access to and integrity of Air Force data throughout its lifecycle. ***(DATA STRATEGY)***	**SMP Links**	**OPR**
Challenge: Airmen require access to data that is consistent and trustworthy to make timely, informed decisions. Airmen regularly report issues with the quality, timeliness, consistency, and accessibility of data. Airmen also lack overarching policies to organize, maintain and preserve data across its entire lifecycle. **Vector**: The Air Force will integrate multi-domain data stewardship, data architecture, and information sharing, to provide a governed approach to data management that is collaborative, disciplined, aligned, well-defined, and repeatable across all security classification boundaries. **Action**: The Air Force will enhance operational effectiveness by developing an enduring data management policy, office and governance processes that provide warfighters with usable, reliable, and value-added data at the right place and the right time.	**AG2.1** **FH2.6** **FH2.7** **ISR.5**	**SAF/CIO-CTO**

GOAL 3: Organize the cyber workforce, and train and educate all Airmen to utilize the cyberspace domain to accomplish the Air Force missions.

ORGANIZE, TRAIN & EDUCATE		
Objective 3.1 – Organize cyber forces to build, operate, secure, defend, extend, exploit and engage in the changing cyberspace environment.	**SMP Links**	**OPR**
Challenge: The Air Force must transform how it organizes to deliver operational agility. Organizations must be adaptive, flexible and responsive to the demands of innovative change and operational priorities. Executing operations and delivering mobile, survivable, flexible and secure communications from command leadership to the tactical edge. This will require flatter, more dynamic and	**AG1.3** **AG1.4** **AG3.2** **AG3.3** **IN1.1** **IN1.2**	**SAF/CIO-A6S**

increasingly diverse organizations with reduced hierarchical, stove piped structures.[18] The Air Force must learn to treat data as an asset in order to conduct information-age warfare. **Vector:** Deliver agile and resilient organizations with supporting authorities, policies and command and control frameworks, and strategic governance that enhance the Air Force's ability to operate in, through and from cyberspace and execute its core missions (REF AFFOC). Optimize organizational structures to support component and command missions. Leverage organizational flexibility, enhanced battlespace and improved planning and assessment to enable self-synchronizing, adaptable, multi-domain command and control to achieve commander's objectives and intent. **Action:** Organize the cyber workforce to execute and assure Air Force core missions in, from and through cyberspace using innovative and effective processes, products, services, technologies, and business models. Emphasize data as a weapon and develop data science as a core skill required to execute Air Force core missions.	**IN2.3** **ISR.5** **ISR.6** **MDA.2**	
Objective 3.2 – Strengthen cyber workforce by leveraging agility, diversity, adaptability, flexibility, collaboration and innovation.	**SMP Links**	**OPR**
Challenge: The Air Force must build an agile cyber workforce capable of meeting the challenges of a high-tempo, information-centric, multi-domain environment. Creating an agile workforce requires flexible approaches to recruiting, development, career and talent management, retention and administration to grow and sustain a workforce that is adaptable, flexible, collaborative, and innovative with the inherent skills and values essential to achieving mission objectives. **Vector:** Attract, recruit, and retain high-aptitude, critical-thinking Airmen with education and skillsets necessary to meet current and future challenges of the cyberspace domain. Develop highly skilled, problem-solving Airmen capable and willing to innovate, collaborate, make decisions under pressure, anticipate threat scenarios, and adapt to fast changing environments. Create an agile workforce with cyber Airmen that are highly proficient in mission platforms, their enabling systems, and the tactics, techniques and procedures necessary for their operation and success. **Action:** Identify and implement innovative options to attract, recruit and retain high-aptitude, critical-thinking individuals across the Total Force (RegAF, Air Reserve Component, and Civilian). Build a diverse, innovative, qualified, flexible and adaptable cyber	**AG1.1** **AG1.2** **AG1.3** **AG1.4** **AG1.5** **AG1.6** **AG3.2** **AG3.3** **GCT.1** **IN1.1** **IN1.2** **IN2.3** **MDA.1** **MDA.2**	**SAF/CIO-A6S** **AF/A2D (OCR)** **AF/A3C (OCR)**

[18] Human Capital Annex, May 2015

workforce to meet the needs of today and tomorrow.		
Objective 3.3 - Enhance cyberspace education and training for all Airmen.	**SMP Links**	**OPR**
Challenge: All Airmen must understand the importance and inherent risks cyberspace poses to the AF core missions and how their actions in cyberspace impacts those missions. All Airmen must understand the need to be proactive and vigilant to protect against cyber threats. **Vector:** Every Airman across the Total Force will understand how their actions impact cybersecurity. Through training and education, Airmen will understand the consequences of cyberspace threats, anticipate and mitigate them through personal and collective behavioral changes and actions resulting in every Airmen equipped with a cybersecurity mindset. **Action:** Transform all academic curricula by embedding cybersecurity into the Air Force lexicon, doctrine and culture. Collaborate with joint, inter-agency and industry partners on best practices and shared challenges to create innovative approaches to cyber education and training for all Airmen. Embed the construct into every DoD institution and reiterate it with strategic communication.	**AG1.1** **AG1.2** **AG1.3** **AG1.4** **AG3.3** **GCT.1** **IN2.3** **MDA.1** **MDA.2**	**SAF/CIO-CISO** **AF/A2D (OCR)**
Objective 3.4 – Increase mission focused cyberspace education and training for cyber Airmen.	**SMP Links**	**OPR**
Challenge: Cyber Airmen must obtain and maintain the skills and knowledge that make them experts, not only in cyber, but also in the Air Force core missions they support.[19] Operational success in the cyber environment requires cyber Airmen with a comprehensive understanding of the mission platforms they operate and sustain, the risks to mission success imposed by system architectures and processes, and the knowledge and determination to recommend and execute changes that mitigate those risks. **Vector:** Train and educate cyber Airmen on cyberspace and its importance to mission assurance of Air Force core missions. The Air Force will minimize the time from requirement to delivery for new cyber training and education needs, and the time investment necessary to complete training and education. The Air Force will institutionalize education on mission assurance and training on functional mission analysis. **Action:** Leverage agile, integrated, and dynamic institutional	**AG1.2** **AG1.3** **AG1.4** **AG3.3** **GCT.1** **IN2.3** **MDA.1** **MDA.2**	**SAF/CIO-A6S** **AF/A2D (OCR)**

[19] Air Force Information Dominance Vision, November 2015

learning centers that are responsive to evolving technologies and capabilities. Consolidate and/or integrate common platform/mission-specific education pipelines. Employ live, virtual and constructive integrated training environments (LVC-ITE) to raise proficiencies, integrate, and increase capacity to develop cyber Airman. Explore viable total force integration solutions to bridge instructional capacity shortfalls. Collaborate with joint, inter-agency and industry partners on best practices to create a comprehensive, shared learning environment.		

GOAL 4 Optimize the planning, resourcing, and acquisition requirements of cyberspace investments.

CAPITAL INVESTMENT		
Objective 4.1 – Formalize and improve Air Force cyberspace enterprise portfolio governance.	SMP Links	**OPR**
Challenge: The Air Force lacks a formal fully integrated cyberspace enterprise investment governance structure today and the various governance structures in use are dis-jointed, parochial, and inefficient. The Air Force must encourage innovative processes, as well as, select, control, and evaluate, and drive Information Technology (IT) and Operational Technology (OT) investments focused on Air Force core mission requirements. **Vector:** The Air Force will build a responsive governance process to manage and govern its entire IT/OT portfolio to deliver new and better capabilities and requirements to assist the acquisition community in delivering cyber resilient weapon systems to the warfighter and increase its return on investment in accordance with Clinger-Cohen Act and OMB TechStat mandated requirements. Collaboration across various organizations and decision-makers is required for effective governance and investment. **Action:** Leverage cross-functional, MAJCOM, CFL, and lead-command teams to develop/institute an agile governance structure and processes that are inclusive, timely and meet Air Force mission requirements. Determine and communicate information technology, requirements, and IT cyberspace investment direction. Hold AF entities accountable to published IT/cyberspace/acquisition policies.	**AG2.1** **AG2.2** **AG2.3** **AG2.4** **AG2.5** **AG3.3** **GCT.2** **INI.3**	**SAF/CIO-A6X** **AF/A2-CIO (OCR)** **SAF/AQ (OCR)**
Objective 4.2 – Develop and Implement a comprehensive Air Force cyberspace and IT portfolio management process.	SMP Links	**OPR**
Challenge: The Air Force does not currently have or use efficient capital planning and investment control, or effective IT portfolio management tools and processes. The Air Force spends $4B to $20B annually on cyber / IT-related systems, and does not manage that	**AG2.1** **AG2.3** **AG2.5** **FH2.1**	**SAF/CIO-A6X** **SAF/AQ**

spend in a single, holistic portfolio view. If we are to deliver better capabilities faster and effectively control IT spending, we must have industry best practice processes and tools in use to inform investment decisions and governance. **Vector:** The Air Force will leverage best practices across all mission areas and functional managers to better manage its overarching information technologies (IT)/operational technologies (OT) portfolio. **Action:** Develop and Implement a cyberspace and IT portfolio management process. Develop and implement portfolio management processes that account for and deliberately co-manage all cyber / IT spends across the various stovepipes. The process must be governed by a formalized investment review board that informs the Strategic Planning and Programming Process (SP3). Ensure IT/OT investments comply with the overall Air Force Enterprise Architecture (EA).		**(OCR)**
Objective 4.3 – Develop adaptable, affordable and agile processes to leverage industry partners to accelerate cyberspace capabilities to the warfighter.	**SMP Links**	**OPR**
Challenge: The Air Force must continually refine, improve, and increase the speed of acquisition to keep pace with dynamic demands of the information environment. Conversely, adversaries operating in the information environment have unconstrained access to technology that provides them with an asymmetrical operational advantage which threatens our national security. **Vector:** The Air Force will leverage idea sharing between government and private sectors. It will leverage talents in the private sector and industry to deliver capabilities through a more agile acquisition process. **Action:** The Air Force will seek new and agile processes to deliver rapid requirements and capabilities to assist the acquisition community in delivering cyber resilient weapon systems to the warfighter. We will leverage industry partners, experimental, innovation, and emerging rapid acquisition vehicles to deliver capabilities with agility and speed. We will proactively prototype capability, and immerse ourselves in over-the-horizon technology that if/when implemented drives costs down and delivers secure and resilient capabilities to the warfighter.	**AG2.1** **AG2.2** **AG2.3** **AG2.4** **AG2.5** **AG3.3** **FH2.1** **GCT.2** **INI.3**	**SAF/CIO-A6X** **SAF/AQ (OCR)**
Objective 4.4 – Unify cyberspace investment requirement priorities across the Air Force within the Strategy, Planning, and Programming Process (SP3).	**SMP Links**	**OPR**
Challenge: The Air Force must proactively identify, plan and program responses to cyberspace capability shortfalls in fiscal year	**AG2.1** **AG2.2**	**SAF/CIO-**

defense planning systems. **Vector:** The Air Force operates in an information environment where change is constant. To counter the emerging cyber threats, we must be postured to dynamically and rapidly respond, both operationally and within the acquisition community. This drives shifts to the AF investment priorities within the AF cyberspace portfolios. Given the dynamic nature of the cyberspace investments, the Air Force must proactively assess the risks to missions, leverage holistic and predictive analysis, and posture adaptive governance processes that are flexible enough to reprioritize resources. **Action:** The Air Force will assess risks to dynamic investments through proactive analysis using frameworks like Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) Cybersecurity Architecture Review (NSCSAR). We will work with DoD, acquisition, and federal partners to seek agile, interoperable, mutually beneficial, combined acquisition programs to deliver IT and cyber capability requirements to assist the acquisition community in delivering cyber resilient weapon systems to the warfighter.[20] Use catalysts such as Defense Innovation Unix Experiment (DIUX) to identify and develop solutions between government and industry to deliver rapid capability to the warfighter.	**AG2.3** **AG2.4** **AG2.5** **AG3.3** **GCT.2** **INI.3**	**A6X** **AF/A5-8 (OCR)**
Objective 4.5 - Achieve efficiencies in IT acquisition and management.	**SMP Links**	**OPR**
Challenge: The Air Force continues to struggle with managing its IT portfolios in accordance with DoD policies due to years of reductions in funding and personnel, leading to instances of unaccounted for equipment and spending. **Vector:** The Air Force will have an IT Asset Management (ITAM) program that will leverage network tools, electronic documentation and workflow, and streamline roles and responsibilities to reduce manpower-intensive manual processes; providing full visibility of our enterprise asset universe and spending patterns. **Action:** Identify policies or procedures that can be changed and areas of IT purchases and management that can be automated to reduce manpower requirements of ITAM in the field and improve the use of systems to manage inventories and maintain compliance with DoD policy. Explore the enterprise-wide use of planning and programming in IT asset purchases.	**AG2.1** **AG2.2** **AG2.3** **AG2.4** **AG2.5**	**SAF/CIO-A6X**

[20] AFFOC, pg 2

Objective 4.6 – Operationalize Air Force Enterprise Architecture (EA).	SMP Links	OPR
Challenge: Strategic Air Force capabilities are developed without integration into the Air Force enterprise architecture. The evolution of warfare requires the Air Force to develop adaptive, interoperable and agile capabilities. The Air Force lacks the ability to view data correlated at the enterprise level and therefore lacks the ability to empirically analyze the complex relationships across mission areas to ensure cost-efficient, agile operations by identifying gaps and overlaps. **Vector:** Leverage the Air Force Enterprise Architecture (EA) and the Cyber Campaign Plan mission thread analysis to ensure interoperability, reduce risk, decrease duplication of effort, and analyze what changes need to be made to meet current and future capability requirements, as well as plan how to align resources to enable those capabilities. **Action:** Establish enduring EA processes to influence investment planning and decision-making by capturing and organizing mission/function data in a consistent and understandable manner to support analyses of alternatives, risks, and trade-offs.	**AG2.1** **AG2.2** **AG2.3** **AG2.4**	**SAF/CIO-A6S**

APPENDIX 1 – TERMS

Air Force Network — The AF's underlying Non-Secure Internet Protocol Router Network (NIPRNET) that enables AF operational capabilities and lines of business.

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)

Cyberspace—A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

Cyberspace Operations—The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP3-0)

Cyberspace Superiority – The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 3-12/JP1-02). The operational advantage in, thru, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference

Defensive Cyberspace Operations—Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called DCO. (JP 3-12)

Department of Defense Information Network—The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security , other associated services, and national security systems. Also called DoDIN**.** (JP 6-0)

Enterprise Architecture – Current 33-401 "The explicit description and documentation of the current and desired relationships among business and management processes and supporting resources (e.g., IT, personnel). It describes the "current architecture" and "target architecture," to include the rules, standards, and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with Government Paperwork Elimination Act, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail." (AFI 33-401)

Flight Plans—Top-level plans that inform resourcing decisions (other than Support Plans), such as MAJCOM plans or functional plans by Deputy Chiefs of Staff, used to achieve alignment across functional areas, influence resourcing decisions, provide informative inputs to Support Plans, or direct discrete activities. They may also be used to develop planning choice proposals. There are no specific requirements directing flight plan development, timeline, or contents but if written, flight plans must be aligned with the Strategy or SMP. (AFPD 90-11, pg. 10)

Information Dominance—The operational advantage gained from the ability to collect, control, exploit, and defend the information environment to optimize decision making and maximize warfighting effects.

Information Environment — The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

Information Technology -- Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is required by a Federal contractor incidental to a Federal contract. Note: The above term is considered synonymous with the term "information system" as defined and used in AF programs. The term "IT" does not include National Security Systems (NSS) according to 44 USC 3502. (AFPD 17-1)

Intelligence—1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities.

Intelligence, Surveillance, and Reconnaissance—An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. Also called ISR**.** (JP 2-01)

Joint Information Environment— 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 CONCEPT OF OPERATIONS, 18 Sep 2014)

Mission Assurance—(Cyberspace)—Measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities. (AF Annex to JP3-12)

Offensive Cyberspace Operations—Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called OCO. (JP 3-12)

Operational Technology – Is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. CIOs with an exclusive, narrow focus on IT must accommodate increasingly overlapping operational technologies system investments, and the groups that manage them. (Gartner IT Glossary).

APPENDIX 2 – ACRONYMS

ADC – Adaptive Domain Control

AF—Air Force

AFFOC—Air Force Future Operating Concept

AFIN – Air Force Information Network

AFNET—Air Force Network

AFPD – Air Force Policy Directive

ARC – Air Reserve Components

C2—Command and Control

CDO – Contested, Degraded, or Operationally Limited Environment.

CIO—Chief Information Officer

CFL—Core Function Lead

CISO—Chief Information Security Office

CMF – Cyber Mission Force

COMAFFORs – Commanders of Air Force Forces

DCO—Defensive Cyberspace Operations

DIUX – Defense Innovation Unit Experimental

DoD—Department of Defense

DoDIN—Department of Defense Information Network

DoDIIS-Department of Defense Intelligence Information Services

EA—Enterprise Architecture

FMA – Functional Mission Analysis

GIISR -- Global Integrated Intelligence, Surveillance, and Reconnaissance

GPS – Global Precision Strike

HAF – Headquarters Air Force

ICS/SCADA –Industrial Control Systems / Supervisory Control and Data Acquisition

IDFP—Information Dominance Flight Plan

ISR—Intelligence, surveillance, and reconnaissance

IT—Information Technology

ITAM – Information Technology Asset Management

JIE—Joint Information Environment

LVC-ITE – Live, Virtual and Constructive Integrated Training Environments

MAJCOM – Major Command

MDC2 – Multi-Domain Command and Control

M&S – Modeling & Simulation

MDOC—Multi-Domain Operations Center

NIPRNET – Non-secure Internet Protocol Router Network

NSCSAR – NIPR/SIPR Cyber Security Architecture Review

NSS – National Security Strategy

NSA – National Security Agency

OCO—Offensive Cyberspace Operations

OSD – Office of the Secretary of Defense

OT – Operational Technology

PED – Processing, Exploitation, and Dissemination

PEO – Program Executive Office

PMR – Performance Metric Review

RDT&E – Research, Development, Testing and Evaluation

RegAF – Regular Air Force

RGM – Rapid Global Mobility

RMF – Risk Management Framework

SIPRNET – Secret Internet Protocol Router Network

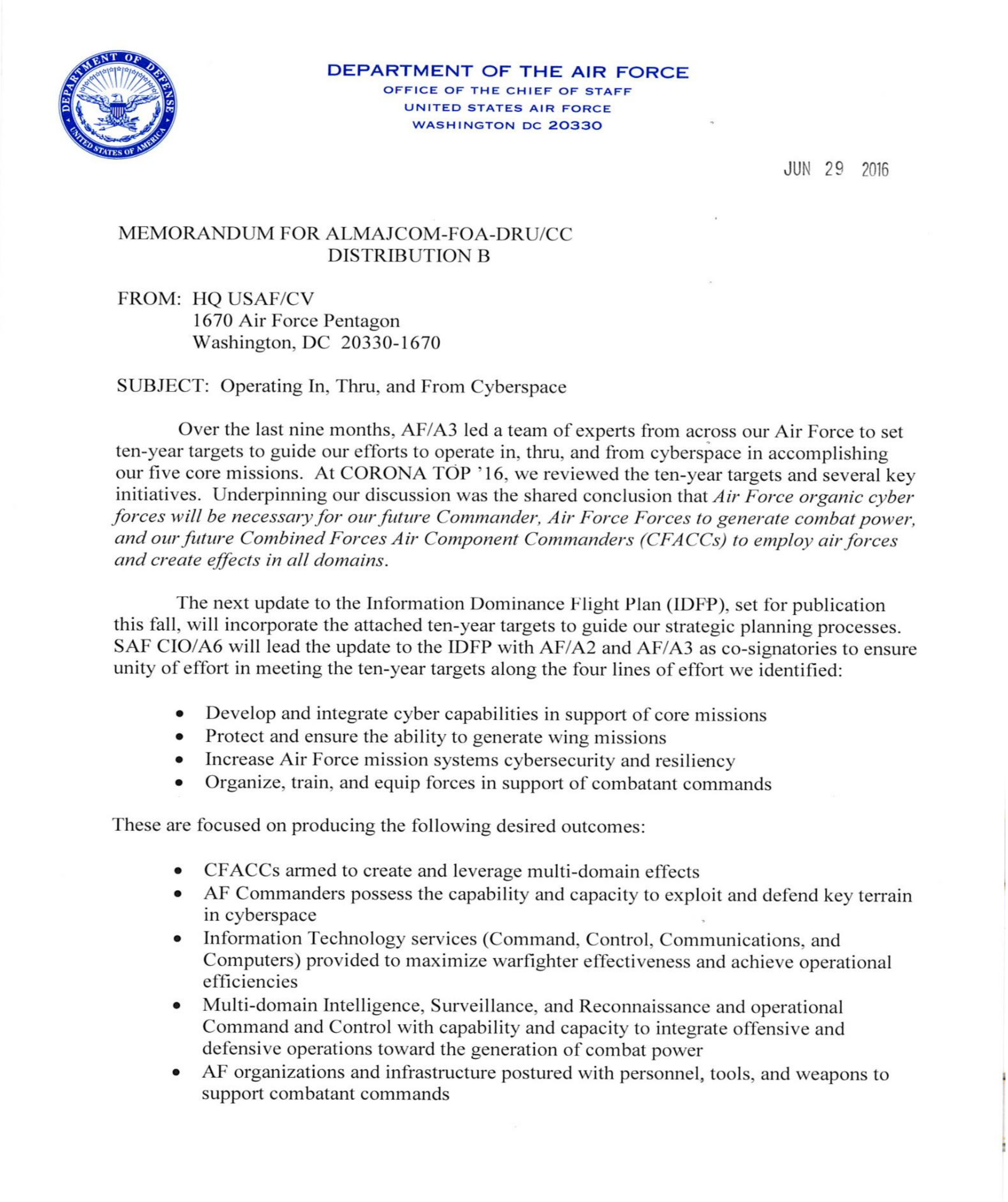
SMP—Strategic Master Plan

SP3—Strategy, Planning and Programming Process

TTP—Tactics, Techniques and Procedures

USCYBERCOM – United States Cyber Command

APPENDIX 3 – OPERATING IN, THRU, AND FROM CYBERSPACE MEMORANDUM



DEPARTMENT OF THE AIR FORCE
OFFICE OF THE CHIEF OF STAFF
UNITED STATES AIR FORCE
WASHINGTON DC 20330

JUN 29 2016

MEMORANDUM FOR ALMAJCOM-FOA-DRU/CC
DISTRIBUTION B

FROM: HQ USAF/CV
1670 Air Force Pentagon
Washington, DC 20330-1670

SUBJECT: Operating In, Thru, and From Cyberspace

Over the last nine months, AF/A3 led a team of experts from across our Air Force to set ten-year targets to guide our efforts to operate in, thru, and from cyberspace in accomplishing our five core missions. At CORONA TOP '16, we reviewed the ten-year targets and several key initiatives. Underpinning our discussion was the shared conclusion that *Air Force organic cyber forces will be necessary for our future Commander, Air Force Forces to generate combat power, and our future Combined Forces Air Component Commanders (CFACCs) to employ air forces and create effects in all domains*.

The next update to the Information Dominance Flight Plan (IDFP), set for publication this fall, will incorporate the attached ten-year targets to guide our strategic planning processes. SAF CIO/A6 will lead the update to the IDFP with AF/A2 and AF/A3 as co-signatories to ensure unity of effort in meeting the ten-year targets along the four lines of effort we identified:

- Develop and integrate cyber capabilities in support of core missions
- Protect and ensure the ability to generate wing missions
- Increase Air Force mission systems cybersecurity and resiliency
- Organize, train, and equip forces in support of combatant commands

These are focused on producing the following desired outcomes:

- CFACCs armed to create and leverage multi-domain effects
- AF Commanders possess the capability and capacity to exploit and defend key terrain in cyberspace
- Information Technology services (Command, Control, Communications, and Computers) provided to maximize warfighter effectiveness and achieve operational efficiencies
- Multi-domain Intelligence, Surveillance, and Reconnaissance and operational Command and Control with capability and capacity to integrate offensive and defensive operations toward the generation of combat power
- AF organizations and infrastructure postured with personnel, tools, and weapons to support combatant commands

In the near-term, there are four key initiatives to continue movement:

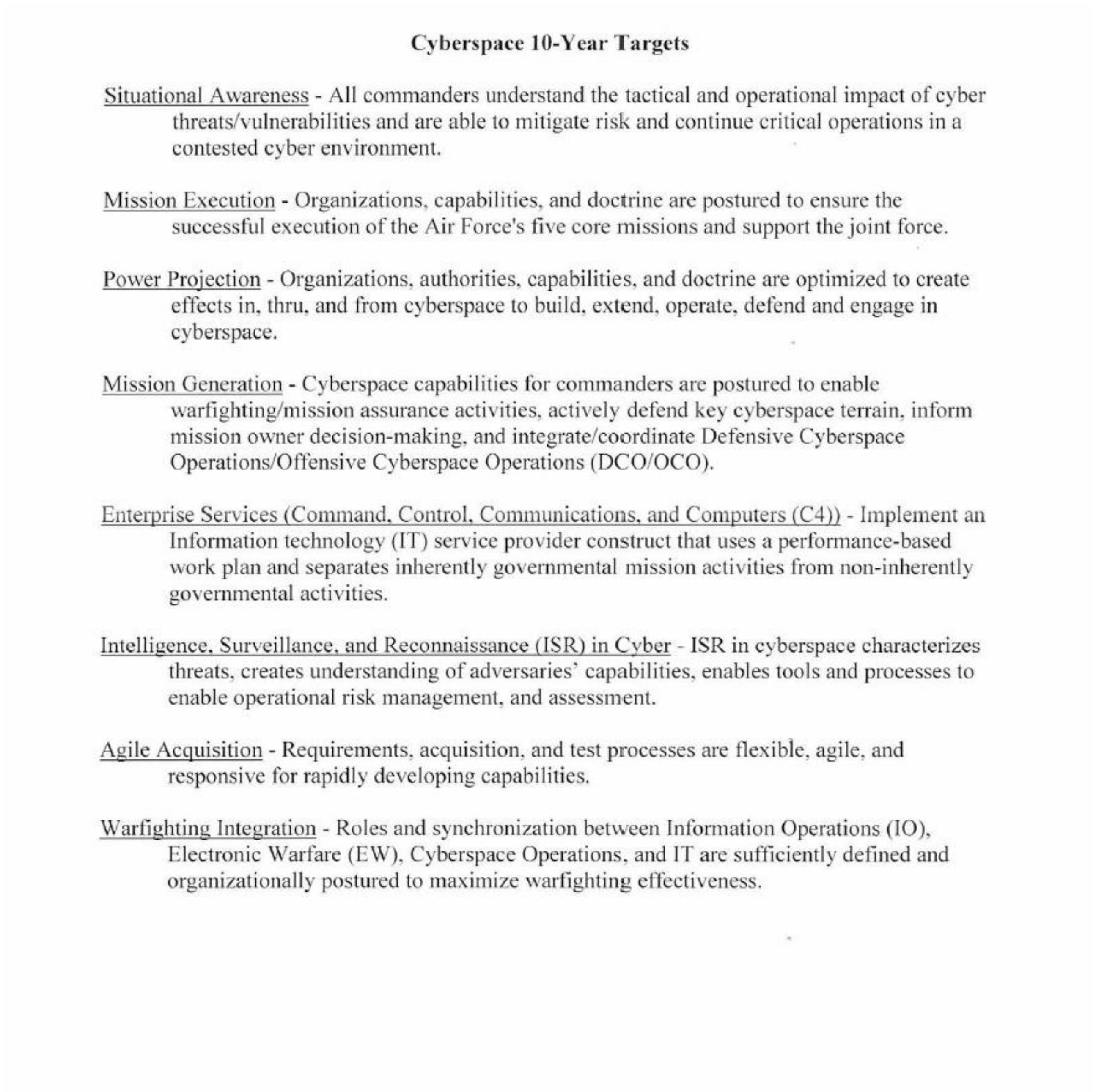
- Assess the current organizational structure for AF cyber forces and provide recommendations to optimize this structure to support component and command missions (OPR: ACC and AFSPC)
- Leverage the Cyber Force Application Future Operating Concept to link planning, gap analysis, requirements, capability development, and readiness to warfighting objectives (OPR: AFSPC)
- Establish Cyber Operations Flight pathfinders within AF wings to provide wing-level expertise to integrate cyber capabilities and identify future cyber requirements (OPR: AF/A3)
- Expand Comm Squadron-Next from the current pathfinders and fully operationalize organizational roles and responsibilities across the Air Force (OPR: SAF CIO/A6)

From squadrons to major commands, our Airmen will operate directly, or indirectly, in, thru, and from cyberspace to accomplish our five core missions successfully. The attached ten-year targets will provide a common aim point as we continue to *Fly, Fight, and Win in Air, Space, and Cyberspace*.

Dave Goldfein

DAVID L. GOLDFEIN
General, USAF
Vice Chief of Staff

Attachment:
Cyberspace 10-year Targets



Cyberspace 10-Year Targets

Situational Awareness - All commanders understand the tactical and operational impact of cyber threats/vulnerabilities and are able to mitigate risk and continue critical operations in a contested cyber environment.

Mission Execution - Organizations, capabilities, and doctrine are postured to ensure the successful execution of the Air Force's five core missions and support the joint force.

Power Projection - Organizations, authorities, capabilities, and doctrine are optimized to create effects in, thru, and from cyberspace to build, extend, operate, defend and engage in cyberspace.

Mission Generation - Cyberspace capabilities for commanders are postured to enable warfighting/mission assurance activities, actively defend key cyberspace terrain, inform mission owner decision-making, and integrate/coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO).

Enterprise Services (Command, Control, Communications, and Computers (C4)) - Implement an Information technology (IT) service provider construct that uses a performance-based work plan and separates inherently governmental mission activities from non-inherently governmental activities.

Intelligence, Surveillance, and Reconnaissance (ISR) in Cyber - ISR in cyberspace characterizes threats, creates understanding of adversaries' capabilities, enables tools and processes to enable operational risk management, and assessment.

Agile Acquisition - Requirements, acquisition, and test processes are flexible, agile, and responsive for rapidly developing capabilities.

Warfighting Integration - Roles and synchronization between Information Operations (IO), Electronic Warfare (EW), Cyberspace Operations, and IT are sufficiently defined and organizationally postured to maximize warfighting effectiveness.