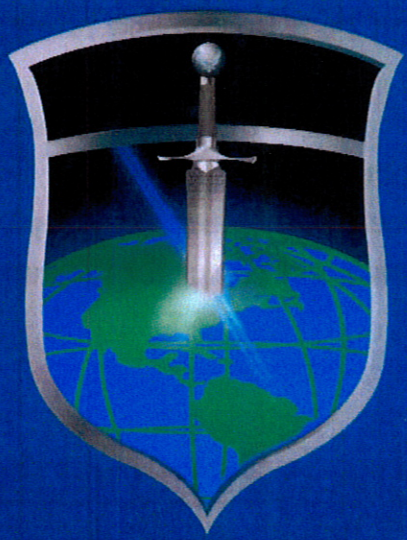
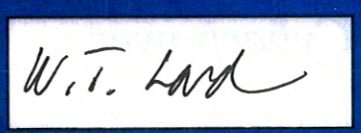


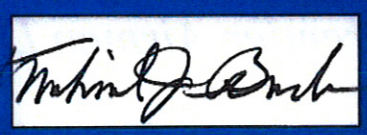




# CYBERSPACE OPERATIONS & SUPPORT COMMUNITY TRANSFORMATION PLAN



WILLIAM T. LORD
Lieutenant General, USAF
Chief of Warfighting Integration and
Chief Information Officer



MICHAEL J. BASLA
Lieutenant General, USAF
Vice Commander, AFSPC

# United States Air Force Mission

*Fly*, *fight* and *win*...in air, space and cyberspace

# United States Air Force Vision

The U.S. Air Force will be a trusted and reliable joint partner with our sister services known for integrity in all of our activities, including supporting the joint mission first and foremost. We will provide compelling air, space, and cyber capabilities for use by the combatant commanders. We will excel as stewards of all Air Force resources in service to the American people, while providing precise and reliable Global Vigilance, Reach and Power for the nation.

# Cyberspace Superiority Vision

*Global Access, Persistence, and Awareness for the 21st Century*

# Cyberspace Operations and Support Community Vision

*Premier Airmen Delivering Unparalleled Cyberpower*

# FOREWORD

The **Cyberspace Operations and Support Community Transformation Plan** is based on guidance found in national, Department of Defense (DoD), and Air Force high level strategies, to include the *Air Force Cyberspace Superiority Core Function Master Plan (CFMP).* This serves to align this plan with high level authority and synchronize the Cyberspace Operations and Support Community's (the Community) transformation with other AF, DoD and federal agency efforts. In the context of this plan, the Cyberspace Operations and Support Community is comprised of the cyberspace AFSCs--17D, 1B4, and 3DX and civilian occupational equivalents--and does not encompass the other AFSCs that are also part of the broader AF cyberspace professional population community. However, the Community will work directly with all key partners to ensure accomplishment of all aspects of the Cyberspace mission.

For example, our strategic objectives, which seek to address the mission change from primarily support functions to the conduct of operational missions, aligns directly to Strategic Initiative 1 of *The DoD Strategy for Operating in Cyberspace*, published July 2011. Specifically, Strategic Initiative 1 directs us to, "Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential." Additionally, the *DoD Strategy for Operating in Cyberspace (DSOC)* identifies five strategic initiatives which can be traced to the tasks and activities contained within this strategic plan. These include the following: the need for an exceptional cyber workforce and rapid technological innovation, the employment of new defense operating concepts to protect networks and systems, and increased partnership with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security.

This transformation plan aligns to the tenets of AFDD-1 and AFDD 3-12 which define Cyberspace Operations and Cyberspace Operations Support. The Community will directly conduct/support Cyberspace missions and provide the IT infrastructure to ensure Cyberspace operations can be accomplished.

The Community transformation goals and objectives also align to the recent guidance published by General Norton A. Schwartz, U.S. Air Force Chief of Staff in the *CSAF Vector 2011*. General Schwartz states the USAF will prepare Airmen for "increasingly contested operations to include bolstering the resiliency of critical physical and virtual infrastructure at strategically vital locations through a combination of dispersal, hardening, warning, and active defense programs." The Community transformation directly supports this statement by developing "continued cyber mission assurance operations and consolidating USAF networks [to] build a passively resilient architecture that will better support future airpower operations."

Cyberspace is a recognized operational domain with command, staff and support functions similar to those of any other domain. This plan is designed to help prepare a specific segment of Cyber operators from the former Communications and Information career-field to transform to an operational mindset and provide capabilities consistent with meeting mission intent within the operational domain of Cyberspace. This plan does not identify or dictate Tactics, Techniques and Procedures or warfighting activities within the Cyberspace domain. SAF/CIO A6 and Air Force Space Command will work directly, and in conjunction, with Headquarters Air Staff A3, A5 and A8 and to ensure the development of Cyberspace Operators will provide the capabilities to meet future mission needs—even as those needs evolve.

The Community transformation also incorporates many of the strategies previously published by some of the key partners in the Cyberspace enterprise. Among the documents that influenced the development of the transformation strategy are as follows: the *Cyberspace Superiority Core Function Master Plan, Functional Concept for Cyberspace Operations* and the *USAF Blueprint for Cyberspace,* published by AFSPC. Additional inputs to the strategy came directly from interviews with senior leaders throughout the cyberspace enterprise, including senior leaders from SAF/CIO A6, AFSPC, and ACC. Detailed information regarding other high level guidance and inputs used to develop the strategic plan can be found in the *External Scan Analysis.* This document surveyed more than 30 sources of information spanning presidential level strategies, DoD directives, official AF documents, publications from sister Services and interviews conducted with senior leaders in the Community.

The Community transformation objectives align to those developed in other high level strategies and guidance. They also incorporate the goals and objectives developed individually by some of the key partners in the cyberspace enterprise. Together, these result in a strategy that will ensure a united and synchronized effort to sustain and develop a highly trained cyberspace workforce. The Community will require input both operationally and functionally from the intelligence and acquisition career fields. Additionally, support from MAJCOMs will also be required to achieve specific acquisition goals/tasks. Therefore, coordination with cyberspace partners is critical to every facet of this transformation plan.

## TABLE OF CONTENTS

## SECTION 1: COMMUNITY TRANSFORMATION VISION

The nature of cyberspace allows for revolutionary ways to approach joint operations. Recognizing these opportunities, as well as the importance of our nation's networks and digital infrastructure, the highest levels of the U.S. government and the Department of Defense (DoD), have identified the development of cyberspace capabilities as a top priority. This emphasis combined with the rapid emergence and understanding of the potential threats in cyberspace, spawned a number of changes within the U.S. Air Force Cyberspace Operations & Support Community *(specifically defined as AFSCs 17D, 3DX, 1B4 and civilian occupational series equivalents in this context)*, the workforce over which SAF/CIO A6 has functional authority. These changes have contributed to the need for a Transformation of the Cyberspace Operations & Support Community (the Community).

To facilitate this transformation, the Community transitioned from a support-based to an operationally focused workforce equipped with the capabilities and training to conduct the full spectrum of cyber operations and support missions to achieve Air Force strategic goals. The Community has numerous roles. For example, the roles and responsibilities of 17DXAs and 17DXBs are distinctly different but are equally important to mission success. This transformation plan will help the Community understand its roles, responsibilities and mission requirements to meet the evolving mission of cyberspace operations by providing a detailed description of the tasks required to realize the Cyberspace Operations & Support Community Transformation Vision. It is a component of the larger Air Force Cyberspace vision of Global access, persistence, and awareness for the 21st Century encapsulated in the **Cyberspace Superiority Core Function Master Plan (CFMP)**:

- Global Access in cyberspace is the ability to establish access to given domains while making possible the delivery of effects across the range of military operations around the world
- Global Persistence is the ability to hold targets at risk and persist with responsive non-kinetic, or along with kinetic effects in, through, or from cyberspace
- Global Awareness is reflected in the ability to sense, maintain awareness and presence, across elements of cyberspace

### Future Environment

*Vast changes will occur to the information and technological environment in which the Community operates and responds.* The Community will provide cyberspace capabilities that foster knowledge-sharing and collaboration within the AF enterprise and across Services and Agencies. This will be accomplished in accordance with the future state vision outlined in the Cyberspace Superiority CFMP, which links the AF Strategic Planning system to National and Department of Defense guidance to ensure supporting investments provide the optimum level of cyberspace capabilities across the range of military operations.

In the future, a foundational change in force structure and doctrine will have taken place within the military and the cyberspace domain. As the Cyberspace Superiority CFMP notes, a smaller, more technologically proficient military has emerged readily networked by fixed and expeditionary sophisticated command, control, communications, computers, intelligence,

surveillance, and reconnaissance (C4ISR). Technological advances allow information to be transported and processed with greater accuracy and speed. This cutting-edge information environment allows authorized users to instantaneously connect with one another, store and retrieve global data, and transform disparate packets of data into decision-quality, actionable knowledge.

The environment is ubiquitous and integrated so that any authorized user, located anywhere in the world, can access desired information via any secure device, regardless of where the information is stored or generated. The environment is intuitive and self-healing. In addition to providing safeguards against unauthorized users to penetrate and manipulate, the environment is able to discern between friendly and unfriendly activities, and quarantine unauthorized activities for further evaluation. The environment is constant and resilient, resistant to natural and man-made events. It routinely run self-checks, identifies system anomalies and degradation, and self-corrects without disruption of services. To aid these future developments, governance processes will be streamlined to ensure that the Community has access to tomorrow's technology today. Additionally, the environment will require a rebalancing of MAJCOM and communications squadrons to meet emerging mission requirements. To advance towards this vision and end-state, our cyberspace capabilities require programmatic actions and strategies to evolve to a future norm of integrated planning, operations and execution.

### Future Mindset

*In the future, every member of the Community will have an operational mindset.* The Community will understand how their individual tasks affect and contribute to missions, the Joint fight, and AF goals and priorities. Moreover, the Community will understand the true impact of their collective roles, responsibilities, and capabilities, and proactively offer solutions to real and perceived problems. The Community will recognize that both its operational and support roles provide equal value to the AF mission and the Joint fight. The shift in mindset will foster an awareness of cross-domain dependencies, which, in turn, will facilitate the Community's ability to be a greater part of operations across all warfighting domains. The Community will know and understand how their talents, roles, and responsibilities support missions and align with AF goals and priorities. By understanding this, they will identify opportunities for growth, gaps in requirements/education/training, vulnerabilities, and develop more effective tools to win in cyberspace.

### Future Education and Training

*In the future, education and training will be on-going and ever-evolving to keep pace with dynamic cyberspace capabilities.* To continue to support the "operational" change in mindset and future missions, education and training will continue to evolve and be much more rigorous, customized, and extensive. Currently cyberspace professionals, including those in the Community, are required to be certified through experience, education and training milestones. The intent is to deliberately develop these professionals throughout their careers. A multi-disciplinary curriculum will teach core competencies including how to establish, integrate, and operate the cyberspace domain across the full spectrum of operations. This curriculum will be designed to develop the technical prowess and ingenuity to exploit opportunities and overcome challenges that lie within the

cyberspace domain. The future Force Development strategy will build on this foundational knowledge, providing the training and experience necessary to develop "Professional Competencies" to officers, enlisted and civilians that are unique to the Community and deliver premier value to stakeholders. To that end, greater emphasis will be placed on strategic thinking and understanding of the Cyberspace domain so that the Community will become more efficient and adept at proactively identifying and solving problems. Additionally, schoolhouses will be among the first to receive new systems and equipment, so that Airmen are trained to use the cutting edge technology they will operate in the field. Also, the force structure for both military and civil service employees will deliver a career track that provides satisfying jobs and produces a cadre of highly skilled and innovative cyberspace professionals regardless of their support or operational roles. Finally, cyberspace training will be on-going and ever-evolving to keep pace with threats and enhancements in cyberspace capabilities.

## Cyberspace Operations and Support Community Future State Core Competencies

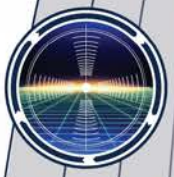
*In the future, the Community will execute and support missions across the full range of military operations, meeting the mission requirements of the Cyberspace capabilities identified in the Cyberspace Superiority CFMP through the core competencies of: Cyberspace Operations, Knowledge Operations, Cyberspace Operations Support, Warfighting Integration, and Governance.* With the new developments in technology and the future information environment, many jobs, tasks, and services formerly provided by Airmen will be automated. Guided by AF priorities, the Community will achieve optimum results from its workforce. As a result, the workforce will work directly with Headquarters Air Force A3, A5 and A8, and be more balanced and better positioned to perform the work that needs to be done in the future. This will maximize the use of personnel and knowledge, and contribute to the AF migration to a Shared Services Enterprise Model. The workforce will be trained to fulfill roles and responsibilities associated with the core competencies and information environment.

**Figure 1. Cyberspace Operations & Support Community Core Competencies**

# CYBERSPACE OPERATIONS


## Decisive Effects

## Integrated Defense



## Real Time C2 & SA

The Community will train and provide the forces that will actively defend and execute cyberspace attacks, in accordance with the operational orders. They will develop the advanced TTPs required to conduct the cyberspace missions identified in the Cyberspace Superiority CFMP: defense, force application, and support. To transition from a support-based to an operationally-focused workforce, the community must provide the capability to perform and provide mission assurance within cyberspace for the warfighter. In turn, these forces will improve the effectiveness of cyberspace capabilities for the following missions: Passive Defense, Defensive Counter Cyberspace, Cyberspace IRS and Situational Awareness, Persistent Network Operations, Data Confidentiality, Integrity and Systems, Cyberspace AOC, Offensive Counter Cyberspace, Contingency Extension, and Influence Operations.

The Community will train the workforce to leverage the enhanced network indicators and sensors to provide commanders 24/7 command and control (C2) and situational awareness (SA) of cyberspace operations for mission execution. Furthermore, the Community will develop cyberspace capability packages, which will allow combatant commanders to select the appropriate effect needed to execute an operation from any necessary physical or virtual location. They will also work with partners in the operational and intelligence Communities, sharing cyberspace domain expertise and in-depth understanding of functional networks across Services and technologies. Thus, within the Cyberspace Operations core competency, the Community will contribute to Cyberspace Superiority by providing a workforce that can deliver a broad range of decisive effects.


## Tailored Enterprise Information

The Community will use the future information environment, and associated information and knowledge processes, to enhance information discovery and delivery across the AF. They will understand the unique information needs of different communities, and how to meet the needs of these communities using the information environment. To accomplish this, the Community will use the information environment to research and develop smart tools for enhancing information discovery and delivery. Authorized end-users will use these smart tools to discover, fuse, and publish secure information. To this end, the Community will consider the terms common to the joint community, and create standard data vocabularies and naming conventions, dynamic indexing, and robust metadata catalogs. These will be linked to systems of record and allow authorized end-users to conduct faster and more expansive searches within the information environment. As a result, end-users will retrieve more integrated and useful search results, which will be prioritized and ranked according to relevancy.

End-users will be able to use smart tools to enhance real-time decision making. The Community will develop intuitive applications for tailoring information displays to end-user needs. End-users will be able to analyze, assess, and sustain the battlefield better by fusing disparate packets of information into a more complete picture. This constant access to well-organized, global information will facilitate real-time informed decisions by allowing end-users to connect with other end-users across Services. Thus, within the Knowledge Operations core competency, the Community--working with Headquarters Air Force A3, A5 and A8--will contribute to Cyberspace Superiority by delivering capabilities that enable tailored and fused enterprise information.

## Enhanced Expeditionary Capabilities

## Seamless Information Environment

The Community will establish and maintain the future information environment, which will be the foundation for all cyberspace activities. This environment will be accessible, seamless, and ubiquitous, so that any authorized user may upload or retrieve global information anywhere in the world, at any given time, via any approved, secure device. The Community will also configure and maintain the necessary infrastructure, equipment, and software to store, modify, and transmit data across the full spectrum of the cyberspace domain. Through this innovative and integrated technological environment all other core competencies will be accomplished.

The Community, along with Headquarters Air Staff A3, A5, and A8, will use this environment to enhance capabilities in executing expeditionary missions. To this end, they will develop communication capabilities to provide near-instantaneous connectivity to meet mission-critical needs worldwide. This will reduce the time to connect and provide near-real time SA in and out of theater, increasing mission timeliness and effectiveness.

## Persistent Network Operations

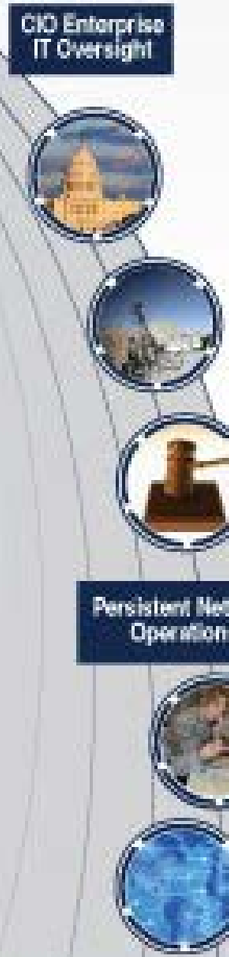
Moreover, the Community and its key partners will develop and implement layered and adaptive defenses based on predictive threat data and analysis received from the intelligence community to protect the future environment. These defenses will allow persistent operations and mission assurance, even in a contested environment, and ensure that the AF can dynamically identify and respond to any on-going attack or system degradation, while simultaneously preserving performance for authorized users. This will ensure that information is delivered as intended and not compromised or manipulated while traversing through cyberspace. Thus, within the Cyberspace Operations Support core competency, the Community will contribute to Cyberspace Superiority by delivering the following future state characteristics: a seamless information environment with enhanced expeditionary capabilities.



In the future, the Community will close the seams between sensors, decision-makers, and warfighters. They will use the future information environment to achieve interoperability and enable the effective exchange of information across Services, systems, and domains. The Community will accomplish this by developing processes and solutions that ensure enterprise C2, warfighter networking, and combat support data management systems can quickly and securely exchange information. To this end, it will develop tools, establish TTPs and standards to effectively use bandwidth and develop systems that automatically adapt to changing connectivity conditions. As a result, warfighters will be able to seamlessly exchange information among integrated space, aerial, and terrestrial networks. This ease of information exchange will improve synchronized and integrated operations by eliminating delays in communication between systems.

Along with faster data processing technology, the standard data vocabularies, dynamic indexing, and robust metadata catalogs will allow information to be more easily synthesized. This will enable timely, authoritative data available to all domains, platforms, and authorized users. Thus, within the Warfighting Integration core competency, the Community will support Cyberspace Superiority by creating an interoperable environment that enables the effective exchange of information.

The Community, along with Headquarters Air Staff A3, A5, and A8, will codify and enforce standards, policies, architectures, and processes to enable AF strategic objectives. These will be used to ensure IT compliance is achieved and sustained for the life-cycle of weapon systems and IT/communications. Compliance will be enforced with a zero tolerance policy. If any system or device is not compliant it will be unable to access the information environment.


The AF Chief Information Officer (CIO) will exercise statutory authority to the fullest extent of the law to support acquisition and contracting/spending reform. He/she will support the warfighter through operationally focused recommendations and inform decisions for IT investments based on enhanced warfighter capabilities supported by enterprise architecture and associated CIO responsibilities. These IT investments will also support the Air Force Space Command commander's vision for a Single Integrated Network Environment.

The AF CIO will change the compliance mindset from "box checking" to understanding the benefits and added value gained through effective IT management processes. This will be accomplished by publishing and communicating, via various means and forums across the AF, the benefits of compliance and portfolio management processes.

Moreover, key leaders across the Cyberspace domain will develop policies in line with their statutory authority that foster smart investment decisions, standardized criteria for IT investment and acquisition, as well as strict enforcement of policies, standards, and procedures. IT portfolio management, and the mechanisms for implementing and enforcing investment decisions, will be adopted by the corporate structure as the singular means to which enterprise IT management will occur. The Enterprise Architecture (EA) will be aligned to AF priorities with flexibility to change with the dynamic AF environment. Enterprise solutions will be developed collaboratively with multiple user communities across the AF to ensure they are timely, mission-focused, and effectively fulfill user requirements. Thus, within Cyberspace Governance, the Community will support Cyberspace Superiority by implementing and enforcing effective standards, processes, policies, and architecture.

## SECTION 2: COMMUNITY TRANSFORMATION STRATEGY

**The Transformation** was created to help the Cyberspace Operations & Support Community transition from a support-based to an operationally-focused workforce. This effort addresses how the Community will meet mission needs and defines the future state characteristics of the five core competencies. This Transformation does not create a strategy for any other AF Community that performs cyberspace missions, but does inform them on the capabilities the Community provides.

To achieve the vision, the Community must have the right mindset and the right tools. This requires that the workforce understands their roles and responsibilities and knows what tools are required to complete tasks. To that end, all roles and responsibilities will be clearly delineated and published so that the Community understands the breadth, depth, and value of their capabilities. Requisite tools will be identified, developed, and provided so that they will be able to perform their assigned functions expeditiously. Moreover, the Community will be regularly trained and educated on how to perform their duties, as well as how to use the proper tools and developing others that will help close operational gaps. Once the Community understands its many roles and responsibilities, they will learn how these roles and responsibilities enable broader effects through kinetic and non-kinetic means to deliver a full spectrum of operational effects. Through this process, the Community will become operationally focused and integrated into all warfighting domains. Accomplishment of the Community Transformation Goals will enable the Community to achieve its future state vision and bridge the gap between today's capabilities and the mindset, environment, and core competencies of the future. The tasks and activities that comprise these goals identify the broad components of processes, people, organizations, policies, and technologies necessary to improve cyberspace capabilities, develop greater cyberspace expertise, and protect mission critical infrastructure.

### COMMUNITY TRANSFORMATION GOALS

The tasks and activities comprising the Community Transformation Strategy are organized around five major goals:

- **Goal 1: Collaborate with Key Partners to Enhance Cyberspace Operations**
- **Goal 2: With CFLI Guidance, Optimize Network Infrastructure and Services**
- **Goal 3: Working with Key Partners, Achieve Interoperability within the AF, between Services, and among Federal Agencies**
- **Goal 4: With Key Partners, Modernize Expeditionary Communications Capabilities**
- **Goal 5: With Key Partners, Strengthen Governance and Compliance**

The tasks and activities comprising these goals are organized into a logical implementation sequence that follows the pattern: Define Requirements; Build Processes; Implement Technology and Enhance Policy; and Educate and Train the Force.

This pattern repeats itself for all of the five goals and presents a logical sequence for synchronizing the implementation of the tasks and activities that comprise the Community's transformation. Because these tasks and activities impact multiple mission areas and future state characteristics, there are strong dependencies and relationships between the tasks and activities contained within and across the five goals.

The pattern for the sequence is based on first defining the high level operational and mission requirements which will guide process development. For many of the areas addressed, there is not enterprise consensus amongst key partners (e.g., AF/A3/5 and AF/A2) regarding the high-level requirements which will guide the implementation of the Community transformation strategy. Once these high-level requirements are solidified, capability and process refinement can begin. It is critical the high level requirements are completed first, because the visions and strategies developed through these tasks and activities will guide the direction of the process, technology, and policy improvements that follow. For some of the tasks, defining requirements includes developing the future state requirements, conducting a gap analysis of current to future state, and developing a plan to achieve the future state. With the solidification of the high-level requirements complete, capability refinement and process improvement work can begin. Once the processes and capabilities are in place, key enablers such as tools, technology, and policy can be developed. Finally, with all the elements in place, education and training of the workforce can be accomplished.

This sequence does not necessarily infer that the five goals must be completed sequentially. Many of the tasks and activities can be executed concurrently, though there are dependency links that cut across the five goals. These tasks and activities will need to be managed carefully to ensure synchronization of effort and to prevent duplication of effort.

## Goal 1: Collaborate with Key Partners to Enhance Cyberspace Operations

### *Key Tasks*

- With Air, Joint, and lead MAJCOM staffs create a unified future state vision for the cyberspace enterprise
- Develop cyberspace operations training plans to ensure Cyberspace personnel maintain a basic competence of Cyberspace operations, certifications and specialties
- Develop Cyberspace domain experts able to plan and execute the delivery of strategic and operational Cyberspace effects
- Develop standardized mission capabilities for both employment and deployment of cyberspace operations and cyberspace support Integrate cyberspace operations into operational planning processes and other AF operational communities
- Align enterprise Command and Control (C2) structure to more effectively integrate with the USCYBERCOM C2 construct
- Collaborate with the other Services and Joint communities to improve the ability to synchronize and integrate cyberspace effects across domains and Services
- Enhance C2 and Situational Awareness (SA) processes to monitor and report the integrity of cyberspace resources thereby providing decision makers with the SA they need to exercise C2 of cyberspace and other operational missions
- Collaborate with industry to enhance technology for conducting cyberspace operations
- Codify cyberspace operational roles and responsibilities and the cyberspace operations and support career field structure

### *Implementation*

Building from the future state capabilities identified in the future state vision, the key partners in the enterprise will develop standardized mission capabilities to employ and deploy cyberspace capabilities. These standardized mission capabilities, presented as a "cyberspace playbook" or "menu of capabilities," will enhance the ability of the enterprise to synchronize and integrate cyberspace operations, while providing visibility of these capabilities to Combatant Commanders. A component of developing these standardized mission capabilities, will be defining the type and combination of forces the enterprise will use to execute cyberspace operations **and support missions.** This includes the development of scalable "Cyberspace Weapon Systems Teams" *(teams include trained people, hardware, software and employment of same)* which will enhance the delivery of services and synchronize operational effects.

With the capabilities defined and the Cyberspace Team construct determined, the key partners can engage in the tactical development of the advanced TTPs which will improve the effectiveness of cyberspace capabilities. This will include the development of Cyberspace "Mission Packages" which will offer scalable and flexible options to commanders. For operations of a more defensive nature, "Hunter Teams" will be formed. These teams will be proactive, employed to locate and mitigate threats and to sweep AF networks for improper use or intrusion by adversaries.

Additionally, pre-approved defensive measures will be developed to allow for the rapid response to an adversary's attempt to disrupt AF networks. Advanced battle damage assessment and analysis techniques will be developed to evaluate the impacts of attacks and allow planners to determine the most effective means to redirect network capabilities around an attack. Advanced network assessment methodologies will be developed to identify, track, and mitigate malicious actors in the network and to distinguish between malicious actions and system anomalies.

Advanced capabilities and TTPs will lead to an improved ability to integrate cyberspace operational planning processes with not only other operational communities, but with other services and Joint communities. As with the development of the future state vision and the advanced capabilities, the close collaboration of the entire cyberspace operations enterprise will be needed. The development of advanced capabilities, such as the "cyberspace playbook" and implementation of Cyberspace Teams, is a precursor to being able to improve the ability to synchronize the planning and execution of cyberspace operations as the development of these improved capabilities has a direct impact on how operations are conducted.

To truly enable these advanced cyberspace operational capabilities, technology will need to be developed. This will be achieved through collaboration with industry. Enhanced technology will strengthen and increase the ability to be proactive in threat detection, by increasing automation of cyber threat identification and characterization capabilities. Advanced tools will continually scan the network to detect possible vulnerabilities. Network assessment tools will be used to counter, minimize, and overcome rogue, as well as organized actors in the AF network, without disrupting mission-critical capabilities. Battle damage assessment tools will provide analysis of cyberspace operational missions.

A major component of the overall enhancement of cyberspace operations is the improvement of the C2 and SA processes used to monitor and report the integrity of cyberspace resources. This will provide decision makers with the SA they need to exercise C2 of cyberspace and other operational missions, improving the overall integration of cyberspace operations. To improve C2 and SA processes the enterprise will need to determine the information requirements decision makers will need, such as disposition of cyberspace forces, mission readiness or availability, and status of networks. Much of these information requirements are dependent on the advanced capabilities being developed. As such, these processes are a key input into the maturation of C2 and SA processes. These mature C2 and SA processes will also be used to increase the overall integration of AF cyberspace with Joint and coalition operations. As such, the means to effectively exchange information at that level will need to be developed. The Community must also identify intelligence requirements to the Intel Community in order to have an understanding/awareness of the adversary's intent, capabilities, and TTPs.

Advanced toolsets will need to be developed to support these mature C2 and SA processes. Ultimately, this information needs to be integrated into the Battlefield COP to truly enhance C2 and SA of cyberspace forces and provide a complete site picture for decision makers. Correlation and

visualization capabilities will support these processes as well, by enabling planners to model and simulate course of actions. This will lead to improved decision making and better synchronization of the cyberspace capabilities.

### Goal 2: With CFLI Guidance, Optimize Network Infrastructure and Services

#### *Key Tasks*

- Define the role, responsibilities & configuration of MAJCOM A6 staffs and base level units
- Identify the mission critical IT infrastructure and systems needed to preserve network services in the event of degradation
- Develop a process for periodically reassessing the mission critical IT infrastructure and systems list against evolving operational requirements
- Adopt appropriate administrative, physical, and technical safeguards to enable simple, secure, streamlined, and effective user access to data and services
- Establish a shared services model
- Expedite IT services delivery procurement/sustainment processes to rapidly deliver technology
- Develop Cyberspace Acquisition expertise and embed personnel in program management offices to ensure systems are fielded interoperable from the first pass
- Adopt or develop smart, mobile hardware and software solutions

#### *Implementation*

Optimizing network infrastructure and services will provide a secure knowledge sharing environment for the AF enterprise. To accomplish this, mission critical IT infrastructure and systems will be identified. Additionally, an AF shared services model must be established. This model should be aligned with the DoD approach for migration of applications and services. Next, appropriate safeguards will be adopted to enable better access to data and services. Expedited processes for the procurement and sustainment of technology will also be implemented. This will be done by analyzing bandwidth usage, establishing standards for effective use of available bandwidth, and partnering with industry to develop tools which automatically adapt to changing conditions in the electromagnetic spectrum (EMS). By engaging with international and federal spectrum management agencies, AF access to the EMS regardless of physical location will be preserved.

Once mission-critical IT infrastructure and systems are identified, the implementation of appropriate safeguards to enable better access to data and services can begin. Security requirements for data, systems, applications, and the network will be refined to incorporate flexible defensive technologies. These technologies will be proactive, as opposed to the predominantly reactionary construct of current technologies. These will be incorporated into the next generation of security suites that will be fielded to enhance security of end-user devices and the overall network. Additional security for access to services, data and platforms will also be implemented. Threat and

vulnerability training will be delivered to all AF personnel to create a stronger "first line" of defense. Role based visibility of system status and diagnostics will also be implemented so that end-users have situational awareness of impacts to normal network services and administrators can quickly diagnose and fix issues. An enterprise wide cyber alert system will also be developed.

Migration to a shared services model has been identified as a key imperative in higher level guidance. To align with this guidance, an AF shared services model will be established. To facilitate the migration, a model must first be evaluated and selected. This will be accomplished with the collaboration of other Services so that a standardized model and a DoD common approach can be developed. Then the AF strategy will be developed, aligned to the DoD common approach. Based on the AF shared services model, an implementation plan for the consolidation of services will be developed and the associated implementation will occur. As part of the implementation plan development, an evaluation of the infrastructure, systems and services will be made to determine what will be removed from AF ownership and responsibility. A key component of the migration to shared services model is the development of an optimization strategy. This optimization strategy will have profound impacts on the workforce as roles, responsibilities, and organizations will evolve to support the shared service model. An optimal balance must be achieved between active duty, civilians, AF Reserve and Guard units, and contractors. The services migrating out of the AF, and the associated infrastructure and systems, will no longer require an organic workforce dedicated to supporting those activities. As such, the workforce will be educated, trained and refocused on other cyberspace functions to ensure optimal use of personnel. The associated career development model(s), roles and responsibilities, and organizational construct will also be updated to reflect the services migrating out of the AF.

Expedited processes for procurement and sustainment of technology will rapidly deliver technology to the field. These processes will be developed through collaboration with the acquisition community as well as internal and external partners. Cyberspace acquisition expertise will also be developed and embedded in program offices to ensure cyberspace requirements are better reflected throughout the full lifecycle of major AF programs. The Community will focus on the sustainment of the network infrastructure through robust life-cycle management of critical IT assets. These processes and process enablers will be used to implement hardware and software solutions that are "smart" and mobile. These solutions will possess transmission capability that is sufficiently sized, reliable and flexible to support diverse mission needs. These solutions will also utilize mobile, ad-hoc network routing techniques and leverage an environment that is more easily accessible. The systems and tools that are "smart" and mobile will enable users to access and integrate relevant, disparate data and enhance continuity associated with position and role transition. This will dramatically improve decision-making throughout all business and mission areas of the AF.

EMS will also be optimized to account for the increasing constraints being placed on EMS availability. Proper accountability of IT assets and the applications and software installed on the

assets is critical for asset management control and for performance of the network and the security of the IT infrastructure. This will be done by establishing standards for effective use of bandwidth, partnering with industry to develop tools which automatically adapt to changing conditions in the EMS, training personnel to develop applications that minimize the impact to bandwidth and ensuring EMS requirements and standards are embedded in the development of Status of Forces Agreements. Engagement with international and Federal spectrum management agencies will also occur to preserve AF access to the EMS regardless of physical location.

### Goal 3: Working with Key Partners, Achieve Interoperability within the AF, between Services, and among Agencies

#### *Key Tasks*

- Develop a common AF and Joint vision to institutionalize warfighting integration (WFI) principles, strategies, and mindset into every requirement, program, system, and service within and across Service core functions
- Align and incorporate WFI principles with Joint doctrine, AFIs and AFMANs
- Formalize process for achieving interoperability within the AF and between Services and other Federal agencies
- Determine a process for utilizing the WFI General Officer Steering Group (GOSG) to further the institutionalization of WFI principles
- Develop processes to enhance information sharing among the AF, other Services, the Joint community, federal agencies, and industry
- Enhance safeguarding and dissemination controls for classified and unclassified information

#### *Implementation*

The starting point to achieving interoperability is creating a vision which will institutionalize warfighting integration principles. The intent is to ensure warfighting integration principles are reflected into every requirement, program, system, and service produced across the AF. This vision will guide the development of formal processes and solutions that will increase information sharing and achieve total integration of space, aerial and terrestrial layer entities and provide warfighters the uninterrupted potential to exploit, defend and conduct force application through Air, Space, and Cyberspace domains with an asymmetrical advantage. Information sharing processes will be enhanced through the development of standardized processes and procedures that allow for self-discovery of information and the creation of intuitive and transparent knowledge-based tools that can be tailored to user needs. This will dramatically improve decision-making across all mission and business areas of the AF. Formal collaboration forums and processes will be developed to provide a venue for AF, Joint, and other national agencies to better partner and communicate. Existing structures, such as the Warfighting Integration General Officer Steering Group, will be leveraged as one of the forums the AF can use to enhance information sharing.

A foundation of these processes will be the implementation of intuitive and transparent data information and management standards. These standards will capitalize on best practices and be developed in collaboration with industry. To enable information exchange, authoritative data sources across DoD will need to be identified. This will allow for the development of DoD standard data vocabularies and a robust DoD metadata catalog, enabling data to be accessed, tagged, and searched regardless of physical location, media, or source. This will lead to timely, authoritative data available to all domains, platforms, and authorized users and enable the development of applications, services, and ontology libraries. This will also provide a robust environment that can be accessed by all mission and business areas to enhance information and service discovery, thereby improving decision making and the day to day execution of processes.

Imperative to warfighting integration is the total integration of space, aerial and terrestrial layer entities across the enterprise. This will be accomplished through the establishment of efforts such as the Joint Aerial Layer Network or the Global Enterprise Network. Another key component of warfighting integration is optimizing the use of available bandwidth. This will be enabled through technology developed in-conjunction with industry that dynamically adapts to changing connectivity conditions to optimize use of available connectivity and provide uninterrupted support to warfighters.

### Goal 4: With Key Partners, Modernize Expeditionary Communications Capabilities

#### *Key Tasks*

- Assess current state of expeditionary communications capabilities and determine requirements for future capabilities
- Develop more flexible and scalable mission capabilities for deploying expeditionary infrastructure and services
- Develop technology to support modernized expeditionary communication capabilities
- Educate and train personnel on new expeditionary infrastructure, capabilities, and technologies
- Develop training plans and adopt more realistic training scenarios for a more modernized expeditionary communication force

#### *Implementation*

In order to modernize Expeditionary Communications capabilities, it is necessary to assess the current state of capabilities and equipment and to determine the requirements for future capabilities. While several improvements have been made in recent years, there are still many capabilities that remain outdated. By identifying gaps between current and desired capabilities, processes and technology can be developed that will provide flexible and scalable mission capabilities. It is imperative to follow the three investment principles identified in the Cyberspace CFMP to prioritize and deliver expected capabilities in support of National and Joint requirements. The rapid deployment of these capabilities will be supported through the organizing of

expeditionary communications assets into scalable and rapidly deployable teams, designed to work hand-in-hand with the UTC generation processes.

Expeditionary Communications capabilities will be supported through the development of highly mobile and portable technology which will allow for expeditionary infrastructure and services to be deployed faster and with a smaller footprint. Collaboration with industry will lead to technologies that virtually and instantaneously establish communication and data transfer capabilities. Additionally, new technologies will be designed to provide maximum flexibility in EMS usage. This will reduce bandwidth and connectivity constraints and ensure continued access to the EMS as forces deploy in and out of different locations. Since the Reserve and Air National Guard will be increasingly relied on to support Expeditionary Communications capabilities, it will be imperative to standardize equipment amongst these units and the active duty force.

Education and training on the new infrastructure, capabilities, and technologies will ensure Cyberspace personnel maintain a basic competence in the full range of expeditionary communications capabilities. Realistic training scenarios will provide the force with the opportunity to maintain their skills and prepare them for challenges they will face in the expeditionary environment.

### Goal 5: With Key Partners, Strengthen Governance and Compliance

#### *Key Tasks*

- Determine the means to more effectively integrate CIO and A6 influence into the corporate processes
- Integrate the Enterprise Architecture (EA) into AF decision making processes
- Develop a plan to continually update the Enterprise Architecture to ensure alignment with DoD and Air Force priorities
- Mature IT Portfolio Management processes
- Develop a customer focused enterprise solution development process
- Conduct a comprehensive review of AF IT systems
- Strengthen and streamline compliance processes

#### *Implementation*

To more effectively integrate the AF CIO into AF corporate processes and better influence IT investment decision making, AF CIO statutory authority must be exercised to its fullest extent. The CIO council can be utilized as a forum to assess the potential impacts of investment decisions, analyzing the potential benefits, costs, and risks. Additional governance structures will also be identified that the AF CIO can influence to exercise its statutory authority. AF CIO will integrate into these structures to ensure investment decisions will be aligned to AF priorities. Along with these governance structures, integration into the processes of corporate budgeting, financial allocation, strategic sourcing, program management, requirements generation, and IT acquisition

processes will be achieved to ensure IT actions are aligned with National, DoD and AF goals and priorities.

Critical to enhancing AF CIO influence, is integrating the EA into the IT investment decision making processes. The EA will be updated to ensure alignment with DoD and AF goals and strategies and to embed interoperability requirements into the EA. The architecture will be open, yet secure, and allow for data to be shared between communities, services, and applications. Updates to the EA will also include aligning sub-architectures to the AF EA. This will facilitate designating the EA as the sole source for evaluating systems and services, as well as assisting in the development of a comprehensive catalog of current capabilities. Once published, this catalog will document system requirements, linkages to strategy, and interoperability requirements for each system and service in the AF. Additionally, a strategy to increase corporate buy-in of the EA will be developed to help educate the other communities on the application of the EA and the benefits it provides, as these are not well understood outside the AF CIO community.

IT Portfolio Management (PfM) will also be a critical element in strengthening CIO governance and in IT investment decision making. The maturation of PfM processes and practices will include developing an IT PfM strategy that aligns to National, DoD, and AF strategies. This strategy will be developed through collaboration with key stakeholders such as AFSPC, SAF/USM, and MAJCOM Portfolio Managers. Relevant objective criteria will be developed to facilitate the evaluation of IT investment decisions. These criteria will be used to assess impacts to architecture, Lifecycle AQ, compliance and resourcing to provide impartial assessments of the potential ramifications of IT system changes or additions.

Tools will be adopted to enable PfM processes. Additionally, a performance measurement system will be developed to measure the effectiveness of PfM processes. This will be vital in institutionalizing the Information Technology Investment Management (ITIM) maturity model and attaining the highest capability rating, Level 5, of PfM.

The development of enterprise solutions, the EA catalog of capabilities, and a comprehensive review of the current IT systems in the AF will complement the PfM processes. The enterprise solutions development process will be based on criteria for a solution being an enterprise solution versus a non-enterprise solution. Then the associated processes for documenting and implementing enterprise solutions will be streamlined. Candidate capabilities will be identified based on the defined criteria for development into enterprise solutions and employ the streamlined processes in the advancement towards full implementation.

Encapsulating all of these changes are the policies and corresponding compliance that codify the processes and associated roles and responsibilities. In order to ensure effective compliance, policies will be updated and the associated compliance will be actively enforced. Compliance processes, which will also have a direct impact on IT hardware and/or components which may not be part of a complete system, will be streamlined to be more efficient and effective, leveraging the

AF CIO influence and integration in corporate processes. Compliance and accreditation will be integrated throughout the IT lifecycle to ensure requirements are fulfilled from initial fielding and sustained throughout the lifecycle of the IT/weapon system. This will ensure that as information and compliance requirements change for the information environment, the applications and systems will adjust accordingly. These information and compliance requirements will be codified in policy as a complete review of AF IT policies will be launched to update the information and ensure security by holding violators accountable for non-compliance. This policy review will also articulate the roles and responsibilities for governing AF IT to add clarity for those charged with this responsibility and for those needing decisions or approval.

## Conclusion

This transformation plan is intended to be an evolving document as the Cyberspace Operations and Support Community continues to transition from a support role to an operational mindset. It will be coupled with an integrated master schedule and strategic communications strategy that will first address how the Communities operational and support roles are of equal importance; speaks to how the Community contributes to the Joint fight, and information environment; addresses both military and civilian force development; determines the proper configuration for MAJCOM staffs and base communications squadrons.

Measures of effectiveness, goals, and timelines to ensure the Community is progressing toward the vision of "**Premier Airmen Delivering Unparalleled Cyberpower**," will be developed to support this plan. Success in attaining progress will contribute to the success of the USAF in enhancing its core competencies and broadening the range of cyberspace expertise to fulfill mission sets across the full spectrum of military operations. The measures of effectiveness account for reaching goals within tightening fiscal constraints as the Community intends to discover, reduce, and eliminate redundant or unnecessary systems, processes, or toolsets to better serve the Air Force.

Throughout the Transformation, the Community will continually work with key partners identified in this plan to ensure the Air Force has the mostly highly trained Cyberspace operations personnel and the capabilities required to meet 21st Century mission requirements in Cyberspace.

ANNEX A: Definitions

| TERM | PURPOSE/DEFINITION | SUPPORTING DOCUMENTATION |
|---|---|---|
| Core Function Lead Integrator | *Lead Airman to plan investment for Service Core Function (SCF) over 20-year period<br>*Builds Core Function Master Plan<br>*Provide agile leadership to help the AF achieve the strategic and operational objectives of the National Defense Strategy with projected resources at the lowest possible overall risk | AFPD 90-11<br>AFI 90-1101 |
| Core Function Master Plan | *Aligns strategy, operating concepts and capabilities by SCF over a 20-year period<br>*Address independent, SCF-related perspectives across the Air Force<br>*Enable a holistic approach to the Total Force Enterprise<br>*Identify mitigation strategies for anticipated fiscal and operational challenges<br>*Prioritize S&T based on far-term strategy<br>*Improve Air Force risk assessment credibility and fidelity<br>*Allow for CFMP Integration to apportion risk among all the Air Force's SCFs<br>*Clarify impact of near-term choices on far-term planning vision<br>*Improve force structure decisions for each fiscal year's Planning Force and Annual Planning and Programming Guidance (APPG) | AFI 90-1101 |
| Functional Authority | Provide oversight and functional advisory services related to functional communities | AFI 36-2640 |
| Enterprise Architecture | Design or "blueprint" that depicts the business components employed in its operations, interrelationships of those components, information flows, and how each component supports the objectives or the strategy of the enterprise. | |
| Portfolio Management | The process of making decisions about IT investment mix and policy, matching investments to objectives, asset allocation, | |

| TERM | PURPOSE/DEFINITION | SUPPORTING DOCUMENTATION |
|---|---|---|
| | and balancing risk against performance | |
| Warfighting Integration | Development of processes and solutions to ensure that enterprise command and control, warfighter networking, and combat support data management systems exchange information and data in support of Joint, Coalition, and AF warfighters | |
| Electromagnetic Spectrum | The entire range of wavelengths or frequencies of electromagnetic radiation extending from gamma rays to the longest radio waves and including visible light | |
| Cyberspace Operations | Cyberspace Operations<br><br>Is defined as the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid (GIG). The Community will train and provide the forces that will actively defend and execute cyberspace attacks, in accordance with the operational orders. They will also assist the operations community in developing advanced tactics, techniques and procedures (TTPs). In turn, these forces will improve the effectiveness of cyberspace capabilities for the following missions: Passive Defense, Defensive Counter Cyberspace, Cyberspace IRS and Situational Awareness, Persistent Network Operations, Data Confidentiality, Integrity and Systems, Cyberspace AOC, Offensive Counter Cyberspace, Contingency Extension, and Influence Operations. | |
| Cyberspace Support | Cyberspace Support<br><br>Cyberspace Support is foundational, continuous, or responsive operations ensuring information integrity and availability in, through, and from Air Force-controlled infrastructure and its interconnected analog and digital portion of the battle space. Inherent in this mission is the ability to establish, extend, secure, protect, and defend in order to sustain assigned networks and missions. This includes protection measures against supply chain components plus critical C2 networks/communications links and nuclear C2 networks. The cyberspace support mission incorporates CNE and CND techniques. It incorporates all elements of Air Force | |

| TERM | PURPOSE/DEFINITION | SUPPORTING DOCUMENTATION |
|---|---|---|
| | Network Operations, information transport, enterprise management, and information assurance, and is dependent on ISR and all-source intelligence. Thus, for Cyberspace Support, the Community will train and provide the forces that will actively defend and execute cyberspace attacks, in accordance with the operational orders. They will also assist the operations community in developing advanced tactics, techniques and procedures (TTPs). In turn, these forces will improve the effectiveness of cyberspace capabilities for the following missions: Passive Defense, Defensive Counter Cyberspace, Cyberspace IRS and Situational Awareness, Persistent Network Operations, Data Confidentiality, Integrity and Systems, Cyberspace AOC, Offensive Counter Cyberspace, Contingency Extension, and Influence Operations. | |

***By doing the work described herein, we will achieve our vision and be ready for the tasks of tomorrow.***