Changing the Way the U.S. Air Force Does IT: A Conversation with Bill Marion, Deputy Chief of Information Dominance and Deputy Chief Information Officer, U.S. Air Force

By Michael J. Keegan

Every Air Force mission depends on information dominance—the operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize war-fighting efforts.

Information that is secure, accurate, reliable, and timely enables information dominance. This provides the war fighter with the best ability to make decisions that outpace their adversary. Innovation alone will not enable information dominance. Rapid and agile acquisition is critical to ensuring IT and operational technology can respond to dynamic cyber requirements.

Airmen need trusted information in place and across the spectrum of military capabilities to conduct their missions. There are many ways for users to communicate and interface among the networks and systems in the information environment; however, the more avenues users have to communicate and interface, the more risk there is for those systems to collect and deliver trusted information.

Bill Marion, Deputy Chief of Information Dominance and Deputy Chief Information Officer, U.S. Air Force, joined me on *The Business of Government Hour* to discuss the mission of SAF/CIO A6, the Air Force's information dominance strategy and priorities, how the Air Force is changing the way it does IT, and much more. The following is an edited excerpt of our discussion, complemented with additional research.

On the Mission of SAF/CIO A6

The Office of Information Dominance and Chief Information Officer (SAF/CIO A6) is responsible for ensuring the U.S. Air Force has developed the governance, guidance, policies, and workforce to allow for the information access, secure communication networks, and decision support tools needed to provide mission assurance in support of the Air Force's core missions. With a portfolio valued at $17 billion, it encompasses everything from normal operations and maintenance to investment areas, all things IT, and all things cyber. Information technology, including cyberspace, is at the core of what the office governs, leads, and manages every day.

The U.S. Air Force's mission is to fly, fight, and win . . . in air, space, and cyberspace. This global mission requires exceptionally well-trained Airmen and sophisticated systems. We support this mission by working to achieve information dominance. As such, the office comprises: CTO (Chief Technology Officer), A3C/A6C (Cyberspace Ops & Warfighting Integration), A6X (Cyberspace Capabilities & Compliance), A6S (Cyberspace Strategy and Policy), and A6Z (CISO – Chief Information Security Officer).

> "Every mission depends on information dominance, but our information advantages are increasingly at risk in a cyberspace environment. Our vision is for the Air Force to fully exploit the man-made domain of cyberspace to execute, enhance, and support Air Force core missions."

On the Air Force's Information Dominance Strategy and Priorities

We describe much of this content in the *Information Dominance Flight Plan*, which is available for those who are interested at www.safcioa6.af.mil.

All Airmen performing missions need information to make the right decisions—whether they're putting bombs on target, dropping humanitarian aid, uploading a software patch to satellite, designing base-level IT infrastructure, or even prescribing the right medical treatment. Every mission depends on information dominance, but our information advantages are increasingly at risk in a cyberspace environment.

Our vision is for the Air Force to fully exploit the man-made domain of cyberspace to execute, enhance, and support Air Force core missions. To meet this aim, we start by defining the three tenets for information dominance.

1. 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

2. 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 to achieve mission assurance across all core missions

3. 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 dynamic cyberspace requirements

We want to increase the effectiveness of Air Force core missions. This means that we need to increase security of Air Force information and systems, as well as realize efficiencies through innovative IT solutions.

We articulate four goals that will move the Air Force toward improving mission assurance and overcoming the challenges posed by "systems-of-systems" complexity and cyberspace vulnerabilities:

- Assure freedom of action and deliver combat effects in, through, and from cyberspace to advance Air Force core missions

- Provide Airmen with trusted information when and where they need it

- Organize the cyber workforce, and train and educate all Airmen to use the cyberspace domain to accomplish core missions

- Optimize the planning, resourcing, and acquisition of cyberspace investments

These goals involve specific priorities that encompass the overall enhancement of cybersecurity, supporting the transition to the Joint Information Environment (JIE). We are also working to transform IT/cyberspace career development and to operationalize authorities and responsibilities.

These priorities are solid. When you look at them, I think they'll morph and change as threats and business objectives change.

On Challenges

I'll identify a few key challenges we are tackling today. They run the gamut but are on some level classic people, process, and technology issues.

Workforce

The number one challenge is the competition for talent. We are not immune to the same issues plaguing the rest of the industry regarding workforce. The competition for prospective workers with the right skills is very tight. I graduated from college during an IT bust. The workforce population was flooded with IT professionals and not many IT-related jobs. Now it's the opposite. There are jobs in cybersecurity, system interface, development, web, mobile, and cloud. There's just unbelievable growth in this area, but not enough properly-credentialed talent available to do these jobs. As a result, we are retooling how we train our current workforce. We are also changing how we recruit. We used to do career fairs, but now we are running cyber competitions at colleges and universities.

Enterprise IT

I would argue we are on a par with Fortune 10 IT companies. Just as a frame of reference, on our unclassified network, we are 700,000 endpoints—700,000 individuals. Our classified networks expand the scope and complexity of our infrastructure. It is not a core competency of the Air Force to maintain PCs or run data centers. These functions are what we call "enterprise IT." We are focusing on outsourcing these functions to industry. We have a big initiative to outsource our web-based office suite, which is ongoing. We also have some cloud solutions that are working marvelously with industry. These cloud migration efforts involve everything from infrastructure-as-a-service to various other platforms. However, migration to the cloud is only one part of a larger initiative within the Air Force. Our transformation of IT isn't just about providing more security, more agility, and more speed. Moving to the cloud allows us to drive the innovation and scalability of the infrastructure, freeing up resources so our workforce can spend more time on cybersecurity business and operations. This, in turn, means better data security and better application security. We hope to leverage the cloud to focus on other key challenges.

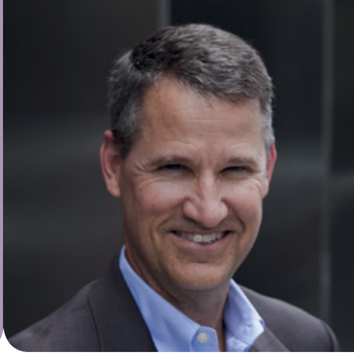
Cybersecurity

Weapon system hardening is a big deal for us right now. We are ensuring those systems are secure, that they operate as we want them to operate, and that data is not being exfiltrated. Cybersecurity is at the forefront. We are focusing on overcoming the challenges posed by our complex systems and networks, and we're confronting cyberspace vulnerabilities. We are working to operationalize an enduring framework identified by the Cybersecurity Task Force to increase cyber support for our core missions. We're doing this by furthering and/or initiating foundational cybersecurity measures.

On Transforming the Development of the IT and Cyberspace Workforce

We are making a concerted effort to retool how we train our workforce. We are bringing on new people and hiring veterans. We are also making sure that when it comes to our current workforce, we are providing the training and skills to match a quickly transforming IT landscape. We need expertise in cloud and agile methodology. In fact, we've been retooling our schoolhouses, moving from waterfall software development to agile. We're retooling the entire curriculum to match a new era.

> "The Office of Information Dominance and Chief Information Officer (SAF/CIO A6) is responsible for ensuring the U.S. Air Force has developed the governance, guidance, policies, and workforce to allow for the information access, secure communication networks, and decision support tools needed to provide mission assurance in support of the Air Force's core missions."



As I mentioned, the Air Force cyber landscape of today is not the same as that of five years ago; the complexities and threats in this environment have grown exponentially—and every Air Force core mission is cyber dependent. Given this reality, we created the Cyber Squadron Initiative. This initiative trains small teams of existing manpower that focus on defensive cyber operations for Air Force weapons systems. The initiative enhances the capabilities of cyber Airmen to defend, assure, and optimize unit missions in, through, and from cyberspace. Currently, fifteen initial cyber squadrons—called pathfinder units—have been organized, trained, and equipped to deploy cutting-edge applications that provide mission assurance to their wing's critical missions. They are being joined by thirty new pathfinder units that have already begun training while identifying their key terrain in cyberspace. Ultimately, pathfinder Airmen will present commanders with a more complete understanding of the risks military operations face in cyberspace. An updated program action directive and policy are to be implemented this year, as well as funding for new training in cyber schoolhouses for officers and civilians enlisted in FY18.

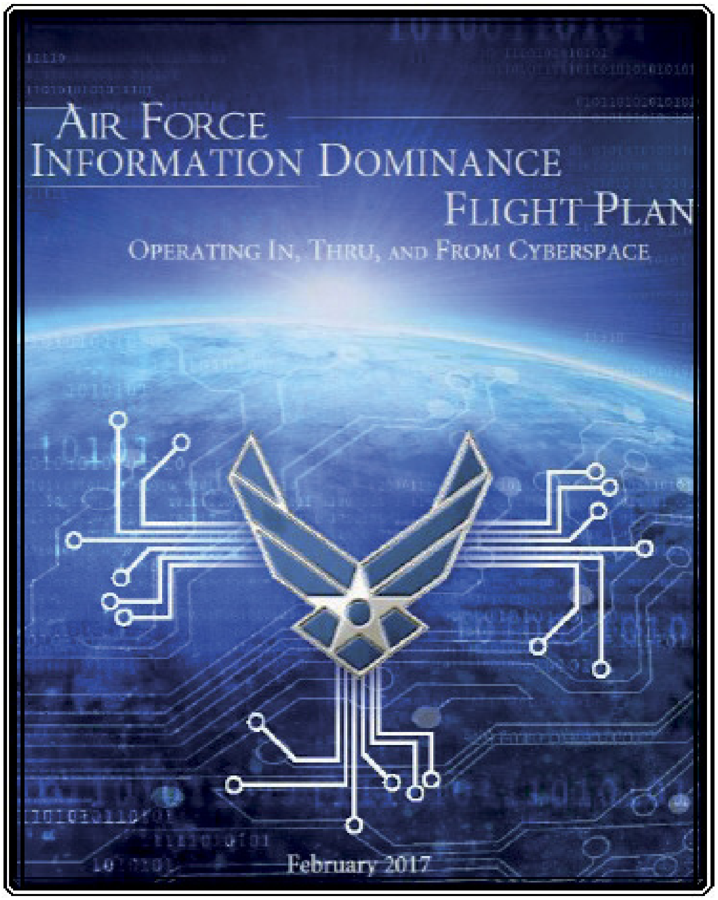
Our readiness is critically dependent upon a properly trained, properly equipped, and well-funded workforce. We will work to recruit, train, and retain those with the necessary skillsets to meet the IT and cyberspace challenges of the twenty-first century.

On DoD Instruction 5000.75 and Its Impact on Air Force Acquisition

The new instruction establishes the policy for the use of the business capability acquisition cycle (BCAC) for business systems requirements and acquisitions. The purpose is to align commercial best practices to minimize customization of commercial products. It was released in February 2017 and represents a phenomenal change in the acquisition mindset.

It was a very collaborative effort. The department engaged the Services to understand the pain points in the process. It posed serious questions as to what adds value to compliance, to security, and to cost-effectiveness. It recognizes that systems acquisition is the joint responsibility of the functional and the acquisition communities. Both communities are accountable for the successful delivery of business capability, from business process design through business system deployment and operations.

The ability to tailor the documentation is key. The authority to proceed (ATP) decision points of the BCAC will be tailored as necessary to contribute to the successful delivery of business capabilities. It was a unique opportunity to review the whole process—to see whether each step or action added value to the acquisition function or to IT procurement.



Source: *www.safcioa6.af.mil.*

We've basically taken an eleven-step process and brought it down to three steps. We can be laser focused on the three steps and make sure they are adding value. We have fundamentally changed the way we acquire IT—getting rid of processes or delegating authority to the right levels. We're on an outreach program right now to make sure that everybody understands there's a new way to do business. One that should be more empowering and offer more flexibility. Most importantly, it also gives us more insight and ability to shape these investments rather than simply following processes and rules that don't add value.

On Collaboration

Collaboration with industry is key. You see this with the outsourcing of our enterprise IT. We also did it with one of our personnel systems. We completely retooled it from an acquisition perspective into a commercial-off-the-shelf (COTS) configuration. We saved hundreds of millions of dollars, cut years off the timeline, and Airmen now get better capability faster and cheaper. Industry collaboration was instrumental in that effort.

On the government side, we collaborate with 18F of the U.S. General Services Administration (GSA), as well as Air Force Digital Services, to innovate and leverage new acquisition authorities. We're collaborating with the GSA on all of our acquisition approaches. It makes a real difference in the way we work.

On Public Service

I didn't go to college thinking about a future career in public service. I came into the federal government as an intern in intelligence—as an IT professional—and I wouldn't change anything for the world. Being an IT professional, I had the opportunity to empower serious missions, protecting our people and the homeland. The sense of service, working on cybersecurity, working in the Air Operations Center, in all facets of the distributed common ground system on the intelligence side, the U2s—these are just unbelievably cool and important missions. There's nothing better. Though there may be the paycheck trade-off, you can go home every day knowing that you helped in some way to protect this country.

To learn more about the U.S. Air Force's Information Dominance Strategy, go to safcioa6.af.mil.

To hear *The Business of Government Hour* interview with Bill Marion, go to the Center's website at www.businessofgovernment.org.

To download the show as a podcast on your computer or MP3 player, from the Center's website at www.businessofgovernment.org, right click on an audio segment, select Save Target As, and save the file.

To read the full transcript of *The Business of Government Hour* interview with Bill Marion, visit the Center's website at www.businessofgovernment.org.