United States Air Force

Presentation

Before the House Armed Services Subcommittee on Emerging Threats and Capabilities

Information Technology Investments and Programs: Supporting Current Operations and Planning for the Future Threat Environment

Statement of
Lieutenant General William J. Bender
United States Air Force
Chief, Information Dominance and
Chief Information Officer

February 25, 2015

INTRODUCTORY COMMENTS

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee this afternoon on information technology (IT) investments and programs. I am Lt Gen Bill Bender, the United States Air Force Chief, Information Dominance and Chief Information Officer. My office is responsible for ensuring the United States 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 five core missions. Our primary mission is to confront and overcome the challenges in defending, while simultaneously leveraging, cyberspace to affect mission assurance. In the first five months in this position, I've decided to act upon my responsibilities by focusing upon four major lines of effort: enhancing cybersecurity, advancing the Joint Information Environment (JIE), developing the Communications and Cyber workforce by transforming career field development, and operationalizing Chief Information Officer authorities. Information technology, including cyberspace, is at the core of what my office governs, leads, and manages each day. I'd like to describe my lines of effort, their relevance to IT within the Air Force, and the critical role they have in assuring the five core missions the United States Air Force must accomplish successfully.

Enhancing Cybersecurity

Freedom of action in cyberspace through the application of mission assurance is a prerequisite for successful Air Force core mission execution. Obtaining and maintaining freedom of action prevents the enemy from effectively interfering with operations. It also

allows the Air Force to deliver more combat power by exploiting cyberspace's unique characteristics. The Air Force will integrate cybersecurity throughout the lifecycle of weapon system development in all mission areas and will focus efforts on keeping information secure. As a man-made entity, cyberspace is fertile ground for game-changing innovation; innovative ideas of our Airmen will be rapidly identified, vetted, funded, and implemented across the Air Force to maximize potential and meet future Air Force needs. Cybersecurity is necessary to achieve these needs.

Thus, cybersecurity is at the forefront of my priorities for IT within the Air Force. I am working to move the Air Force toward overcoming the challenges posed by our complex systems and networks and confronting cyberspace vulnerabilities. The Internet Society, a non-profit entity dedicated to keeping the internet as an open platform, estimated that in 2015 there will be three billion internet users worldwide. CISCO Systems, Inc., estimates there will be 15 billion internet-connected devices by this year. Each internet connected person and device represents a potential vulnerability to cyberspace. We must understand and confront the reality that a contested cyberspace affects our wartime operations and opens our aircraft and systems to vulnerabilities.

To confront this issue, I have convened, under the direction of the USAF Chief of Staff, the Cyber Task Force. Several Air Force organizations are working this issue, but what has been missing is an enterprise level coordination and approach to provide solutions. This task force teams us with our operations and intelligence teammates to integrate efforts across the Air Force and focus on concrete action steps to mitigate our risks within cyberspace. This task force will not only work to define the threats and vulnerabilities, but also provide a risk management strategy and the needed actions and investments to

implement them. The focus of this task force is to recommend steps to provide mission assurance in a contested environment: mission assurance, not system assurance.

Joint Information Environment

Cybersecurity also drives one of my other lines of effort: enhancing the Joint Information Environment. The Air Force will achieve greater collaborative efficiency across the DoD and with external mission partners by bringing Air Force IT architectures, systems and processes into compliance with the Joint Information Environment (JIE). We will leverage opportunities to manage information and develop a data management plan to ensure data veracity as well as the accessibility of information to mission users. This ambitious effort to align, constructs, and defend our networks aims to provide better information access for users. JIE will help deliver mission assurance and provide warfighters and our mission partners a shared IT infrastructure. It will leverage networks with common configurations and enterprise services within a defendable single-security architecture. JIE will help protect the integrity of information and increase the ability to respond to security breaches across the enterprise. Air Force core missions benefit from all of these actions through greater operational and technical resilience, improved interoperability and effectiveness, enhanced integration across information systems, faster capability delivery, prioritized secure capabilities, and reduced costs. Ultimately, field commanders will benefit the most from JIE; they will be able to integrate information technologies, operations and cybersecurity to meet today's fast-paced operational conditions.

Now is the right time for the Air Force to become a full, aggressive partner in ensuring progress towards this concept. This is a multi-service effort and the DoD CIO is

moving forward; however, we must ensure every Service is committed to the effort, including in their budget, and that JIE is aligned in their Service priorities.

Revolutionize IT/Cyberspace Workforce Development

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

Our readiness is critically dependent upon a properly trained, equipped, and funded workforce. We will work with DoD efforts to recruit, train, and retain those with the necessary skillsets to meet the IT and cyberspace challenges of the 21st century.

Operationalizing CIO Responsibilities and Authorities

This office has taken great strides in aligning authorities and the organization to support warfighting integration across all Air Force mission areas. We are integrating cyberspace strategy, policy and programming across the mission areas, Air Staff, and lead command units in the field. This effort aims to provide the right information to the right people at the right time. By fostering the flow and sharing of information, we are working to improve combat execution.

Investments and spending on cyberspace capabilities across the Air Force must be fully transparent and aligned with supporting mission assurance. Improved spending alignments will provide additional resources for modernization and further innovation. My office will assist programs that acquire cyberspace and IT capabilities at earlier and more varied stages of the acquisition process than it does at present. This will improve responsiveness, unity of effort, and the Air Force's ability to implement best practices in cyberspace/IT investments.

However, we must understand that IT investments are the price of doing business in the 21st century. We cannot delay investments and deliver outdated technology and capabilities to the field. We must work to refine acquisition processes to make more timely decisions and deliver the latest capability to the field.

For example, the tools involved in reporting financial data are complex and mystifying. We manually input information into one repository, upload spreadsheets into another system, and enter additional data into a third database for the AF Corporate structure. The Air Force submission process is a maze of steps across four organizational hierarchies. The Presidential Budget cycles involve several actions and many actors over a short timeline.

These processes are dependent upon dissimilar systems from the respective services to those at the OSD and DoD levels. In order to deliver current IT capabilities to the field, these complicated processes need an overhaul. A roadmap and plan for this OSD and Service integration activity needs to be accomplished. The output would be a more expeditiously reported IT Budget with greater fidelity.

My office is fully aligned with executive measures to improve IT management and acquisition. Effective federal IT acquisition requires thorough knowledge of the federal acquisition system, a deep understanding of commercial IT capabilities, and the unique challenges inherent to successfully delivering large IT programs within limited time constraints. Our office is committed to the development of project management (PM) and IT skills within the workforce; and we're working to determine the proper placement, certification, and use of personnel as program managers of IT systems.

Conclusion

Delivering IT and cyber capabilities to the warfighter so they can provide mission assurance is absolutely critical to our national security. Our lines of effort outlined above will help deliver personnel, capabilities, and resources that provide greater mission assurance. We look to provide needed IT and cyber improvements and make the most efficient use of financial resources. I thank you for the opportunity to address this subcommittee. I thank you for your interest in, and leadership on, these critically important IT and Cyber-related issues, and I look forward to your questions.