DEPARTMENT OF THE AIR FORCE

BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
UNITED STATES HOUSE OF REPRESENTATIVES

SUBJECT: CYBERSPACE AS A WARFIGHTING DOMAIN: POLICY, MANAGEMENT AND TECHNICAL CHALLENGES TO MISSION ASSURANCE

STATEMENT OF: LIEUTENANT GENERAL WILLIAM L. SHELTON, USAF
Chief, Warfighting Integration and Chief Information Officer

5 MAY, 2009

NOT FOR PUBLICATION UNTIL RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRIORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
U.S. HOUSE OF REPRESENTATIVES

LIEUTENANT GENERAL WILLIAM L. SHELTON, USAF

Chief of Warfighting Integration and Chief Information Officer

United States Air Force

Good afternoon, Chairman Smith, Congressman Miller and distinguished members of the subcommittee. I am the Chief of Warfighting Integration and Chief Information Officer (CIO) for the U.S. Air Force and I am pleased to appear before the subcommittee today to discuss our efforts to address the challenges in the cyberspace domain.

Organizing the Force

Several years ago, the U.S. Air Force recognized the growing importance of cyberspace. On December 7th, 2005, we took the unprecedented step of adding cyberspace to our mission statement, and placed that domain on an equal footing with our more traditional operating environments of air and space. Since that time, we have been moving forward to organize, train and equip our Air Force to operate in cyberspace for joint operations.

As we moved into this new domain, we realized we would need to establish a new organization focused on developing expertise and optimizing capabilities in this arena. The Air Force decided to leverage and integrate Air Force Space Command's existing organizational responsibilities and present forces to United States Strategic Command via a new Numbered Air Force.

On February 20th of this year, the Secretary of the Air Force (SECAF) approved the activation of Twenty-fourth Air Force (24th AF), organized under Air Force Space Command (AFSPC) and a component under United States Strategic Command (USSTRATCOM), to serve as the focal point for Air Force cyber operations. Once activated, 24th AF will support USSTRATCOM and other combatant commanders to operate in, through and from cyberspace, integrated across all operating domains. The 24th AF will bring together existing Air Force cyber operational capabilities under one commander, allowing the Air

Force to better support the larger effort of USSTRATCOM's Joint Functional Component Commander for Network Warfare. Additionally, the 24th AF Commander will command and control Air Force Network Operations (AFNetOps), providing a centralized command structure for operations and defense of Air Force networks and protection of Air Force information residing on the network across the Air Force portion of the Defense Department's Global Information Grid (GIG).

The 24th AF will be comprised of three subordinate Wings: the 688th Information Operations Wing at Lackland AFB TX, dedicated to counter-information and information operations; the 689th Combat Communications Wing at Tinker AFB OK, responsible for extending and sustaining the Air Force portion of the GIG into the theater of operations in support of geographic combatant commanders; and the 67th Network Warfare Wing at Lackland AFB TX, responsible for conducting network operations in cyberspace as directed by the Commander, USSTRATCOM.

The Air Force is still in the site selection process for 24th Air Force headquarters. We are conducting an extensive review to ensure the site selected is the best possible location to ensure success of the 24th AF. Once a final location is determined, the Air Force is poised to activate 24th AF as soon as practical.

AFSPC will be the Air Force's lead Major Command to organize, train and equip our Air Force cyberspace forces. As part of this effort, significant resources and responsibilities are being administratively transitioned to AFSPC including the Air Force Information Operations Center, the Air Force Communications Agency (which has been re-designated as the Air Force Network Integration Center), the Air Force Frequency Management Agency and the 38th Engineering Installations Group. AFSPC will also assume functional responsibility for technology insertion efforts, project management, engineering and installations, communications maintenance, expeditionary communications and AFNetOps. As the Chief of Warfighting Integration and the AF CIO, I will retain the responsibilities for Air Force communications and information policy, guidance and oversight.

The National Defense Authorization Act (NDAA) of 2009 mandated the Air Force establish a Chief Management Officer (CMO) with overall responsibility for transforming business and combat support operations in the Air Force. We have made solid progress defining the role of the CMO, and recognize the clear relationship between that office and the CIO. We are currently balancing the Information Technology (IT) responsibilities and accountabilities of the CMO with those of the CIO, as directed by the Clinger-Cohen Act.

Additionally, SECAF has delegated the Freedom of Information Act (FOIA) responsibilities to the CIO. With this delegation, we instituted new processes and deployed a new interface to the public -- eFOIA. This "electronic face-to-the-public" web-based system streamlines the request process and improves tracking and overall responsiveness. As a commitment to continuous improvement and responsiveness to requests for public release of information, we reduced FOIA backlog requests by 17% in FY08, and are working on additional improvements to continue backlog reduction in FY09.

Training the Force

As we organize ourselves to operate efficiently in the cyber domain, we are tackling the challenge of increasing the size and expertise of our workforce. Issues we face include recruiting, training, incentivizing and retaining the increasingly scarce technical talent in our Nation. Despite the economic downturn, the competition for these people remains fierce. We are working hard to recruit the cyberspace warriors of tomorrow and to retain the great people we have in these positions today.

The current Air Force communications and information community is made up of over 60,000 personnel with 31,000 active duty personnel, 18,000 civilians and just over 17,000 Guardsmen and Reservists. We train about 185 new active duty communications and information officers per year, and about 155 students from the Guard and Reserve, international allies and government civilians, for a total of approximately 340 students per year. We also assign officers with relevant pre-commissioning

educational and/or life experiences to appropriate positions to leverage those skills to support this emerging mission.

Recent force reductions, combined with enabling technological change, have driven us to retool our enlisted workforce. We are consolidating 15 enlisted specialties into 11 career fields. Technology has enabled us to consolidate similar competencies into single vocations and in turn establish several new vocations focused on security and personal services delivery.

To ensure our personnel are well-trained before assuming their initial positions, we have modernized our pipeline training courses. We are considering additional training they should receive and at what point during their career they should receive it. We expanded our distance learning capabilities, and broadened our academic education program. We are updating our Professional Military Education courses to include cyber security, adding a cyber security block at Air Force Basic Military Training, and continuing to develop an advanced degree program at the Air Force Institute of Technology (AFIT) at Wright Patterson Air Force Base, Ohio. We are also working with our joint counterparts to take full advantage of the excellent cyber training capabilities at Corry Station, Pensacola, Florida.

After investing this much training in our people, we must extend our best efforts to retain them. Selective re-enlistment bonuses, as well as military benefits, are helpful in this regard. Air Force benefits compete well with industry, so we are hopeful the mission, the Air Force culture and the incentives will help us retain the best and brightest America has to offer.

The Government Accountability Office reports that a significant percentage of civilian personnel are, or will be, retirement eligible in the next 10 years. We believe our civilian workforce, who serve alongside their uniformed colleagues, is crucial to our success in this domain. A strong civilian development framework will attract new personnel to public service to fill the vacancies from the retiring workforce. We are working to identify key leadership and developmental positions and will

codify policies to manage these positions to ensure we deliberately develop people throughout their careers.

Like many others, I am concerned about the decreasing number of engineering, science and mathematics graduates from our nation's colleges. To assure our success, the Air Force will continue to need officers and civilians with technical educational backgrounds. The waning interest in science, math and technology, coupled with the rising demand for private sector IT and engineering professionals, will challenge our ability to attract, recruit and retain technically qualified military and civilian personnel. We believe this is not just an educational issue or an issue of competitive advantage. Maintaining a robust foundation of educated and trained technical professionals is a National Security issue.

Equipping the Force

The Air Force investments in IT reflect the priorities and direction of both the joint community and our Service leadership. To meet the challenges of rapidly advancing technology, we are restructuring our processes to acquire information technology. Traditional structures designed to purchase major weapons systems, with long attendant development cycles, are ill-suited for the fast-paced IT world where technologies can often be rendered obsolete in a matter of mere months. We are streamlining our processes to shorten the requirements-to-capability-delivered timeline through the use of commercially available technologies, leveraging open source technologies and exploiting opportunities to rapidly field prototype efforts.

The National Defense Authorization Act for Fiscal Year 2005 (NDAA 05) stated that defense business system modernization investments greater than $1 million must be approved by the appropriate OSD Investment Review Board and Defense Business Systems Management Committee. This was an important Act for the Air Force. Using this direction, combined with increased senior leader emphasis, we are conducting reviews of our investments. Since NDAA 05 was enacted, we have successfully certified 62 business systems. As we matured the review process, we identified

opportunities to streamline other processes. During FY07, my team developed a framework to review all statutory requirements across IT systems providing the Air Force with a single-point review of all IT systems on an annual basis.

We established a process to execute similar reviews on non-business systems. This initiative provided a unique opportunity for the CIO and acquisition community to combine reviews and eliminate duplication. This consolidation ensures all critical IT investments are formally evaluated either at an acquisition milestone, or another annual review.

This realignment also yielded other successes in IT management. We updated our portfolio investment review process to coordinate decision-making with other business enterprise management components. The new process generates an IT investment strategy that is linked to the budget cycle, and aligned to Air Force strategic objectives. Last year, we published an Air Force Instruction that formally establishes the guidelines, policies and procedures for approving and managing Air Force IT.

Today we are managing our IT certification and accreditation process to ensure that appropriate security controls are in place prior to integrating an IT system on the Air Force network. Specifically, the Air Force established robust goals for FY09: first, compliance rates of 95% or higher for certification and accreditation; second, validation of current annual security reviews, security controls and contingency plan testing; third, completion of Information Assurance (IA) Awareness training; and finally, submission of a Plan of Action and Milestones to the CIO that formalizes these policies. Compliance metrics have been developed and are tracked weekly by the Air Force Senior Information Assurance Officer who reports directly to me.

Protection of our critical information is vital and we have instituted measures to ensure the security of personally identifiable information, to include all military, civilian and public affiliation data. Restricting the disclosure of personal information is a top priority, resulting in an initiative to reduce the use of Social Security numbers. Additionally, we annually review our IT investments and identify

systems that collect or generate personal information. We use this data to ensure we have appropriate safeguards that are documented, verified and approved by me. To date, we have completed 85% of this requirement and will continue to improve this rate throughout the year.

While we have achieved much, we are committed to constantly improving our governance process to support new and on-going acquisition efforts. Partnering with our DoD acquisition team, security is a critical enabler in the development of new systems. We will no longer "bolt-on" expensive security options onto our systems; rather, we will integrate services to achieve dramatic security improvements. The AF is dedicated to improving operational effectiveness and increasing efficiency through governance and leadership. We will do this through our enterprise architecture, deliberate processes and cultural change.

With our improved processes and governance measures in place, we are now focusing our investments in a few critical areas reflecting our priorities. To help reinvigorate the Air Force nuclear enterprise, we will continue to provide dependable and secure command, control, communications and information for our nuclear forces. We are modernizing our already reliable cryptographic program to ensure the continued security of vital nuclear assets.

By partnering with joint and coalition team members, we will build networks that guarantee the security of data in any environment, while ensuring the necessary data is shared appropriately across domains. Our long-term goals are centered around our support to the joint efforts to enhance the GIG. The Public Key Infrastructure (PKI) ensures front-line security for information systems and applications on the GIG and provides critical user protection across the Department of Defense, as well as our contractors' networks. Our continued priority is to modernize and develop the proper safeguards to secure our data in both a joint and coalition environment. As we continue to deploy with our service and coalition partners, it becomes increasingly important to ensure we can communicate effectively with the entire joint and combined team, while maintaining the security of our information.

The SECAF and the Chief of Staff of the Air Force (CSAF) recently directed the Air Force CIO to take a strong and centralized approach to network management. With guidance from the Air Force Senior Acquisition Executive, Air Force Space Command and the Senior Working Group, we are developing an end-to-end IT governance policy. This combined effort, will take control of the Air Force enterprise architecture. It will create a "build-to-design" network governance structure, based on an enforceable architecture that will ensure security and reliability, while reducing development costs. This policy will also enable the AF to align network operations command and control capabilities to the joint network command and control structure to ensure both security and performance of network components.

My organization has undertaken a significant design effort to align with DOD's Net-Centric Data Strategy. We call this effort the Singularly Managed Infrastructure with Enterprise Level Security or SMI-ELS for short. SMI-ELS addresses two critical mission needs. The first (SMI) is the sharing of information across Air Force, DOD, US Government and Coalition networks. The second (ELS) is the protection of Air Force information and the infrastructure that enables the sharing of that information. SMI-ELS will provide us access to mission critical information via a secure, robust infrastructure which will protect Air Force users, information, and technical resources from both internal and external threats. To drive the Air Force to higher degrees of information and knowledge-based operations, SMI-ELS will span enterprise-level business processes such as architecture and acquisition, technical solutions networks, web services, applications, data repositories, computing infrastructure, and force transformation.

Modernization and standardization of network equipment under the Combat Information Transport System (CITS) program provides our Airmen with the necessary tools to centrally operate, defend and manage the AF network. An example I would point to is the Expeditionary Combat Support System (ECSS) which allows the AF to modernize and consolidate, or turn off, expensive, legacy logistic

systems, generating significant future cost savings. ECSS also provides accurate, timely decision support across the supply chain.

Perhaps the most significant challenge we face is the constantly evolving nature of the threat in cyberspace. Threats in cyberspace move at the speed of light, and we are literally under attack every day as our networks are constantly probed, and our adversaries seek to exploit vulnerabilities in our network enterprise. To keep pace with the efforts of our adversaries, we need a robust research and development effort to keep us ahead of those who would seek to damage our information networks. I have two particular areas of concern regarding challenges in the defense of our networks; generally both R&D topics have received national level attention through the Comprehensive National Cybersecurity Initiative (CNCI) and are being reviewed as part of the Administrations 60-day Cybersecurity review. The Air Force will ensure its R&D is consistent with these broader USG efforts, while maintaining specific R&D capabilities to ensure mission essential functions. The first is our ability to command and control our network infrastructure and have full situational awareness of the activities taking place on that network. This is an area that will benefit from government-sponsored research and development. To date, our reliance on commercial efforts poses a challenge of scalability. The scope of effort required to defend the Air Force and DoD enterprise far exceeds that of the traditional commercial customer. We are continually faced with the challenge of adapting and employing tools that are not appropriately sized for our enterprise needs. This leaves us with an incomplete view of the activities on our networks and a limited ability to execute the real-time responses required to preemptively respond to the threat. R&D efforts need to focus on developing tools that allow our cyberforce to see, know and act in the same unified way as our military forces do in every other modern battlefield domain. The second area of concern is our ability to respond to specific malicious threats, such as viruses, a problem that is not well suited to traditional R&D. While DoD conducts some organic research in response to specific cyber threats, we rely heavily on the day-to-day efforts of industry. In

most cases, this approach does not keep pace with the cyber threat; instead, it is reactive in nature. The threats can bypass defenses with minor modifications—often the case with computer viruses.

As a final thought in this area of equipping the force, we are working to assure relevant, timely and secure information to the joint warfighter engaged in combat operations overseas. In support of an urgent request from US Central Command, we deployed a capability referred to as Battlefield Airborne Communication Node (BACN). This new capability enables data translation and forwarding that connects legacy data links to emerging capabilities. BACN also increases the range for voice communications beyond line of sight through the use of radio frequency translations and repeaters, achieving both voice and data link interoperability without modifying our current equipment or aircraft. This range extension capability ensures early radio contact so we can transmit targeting information to strike aircraft like the B-1, allowing a first-pass strike, and avoiding the previously required overflight of the target area that often alerted enemy forces. The high altitude at which we operate allows us to avoid enemy small arms fire and overcome line of sight "shadows" experienced by aircraft flying low in mountainous terrain.

Since, October 2008, BACN has supported close air support, convoy, time sensitive targeting and air drop missions with great success. Based on over 700 troops-in-contact situations, we have seen a 25% reduction in the time it takes for ground units to establish communications with close air support aircraft. This improved speed of establishing communications has also enabled a 45% increase in kinetic results—bombs on target in support of our ground forces. Our efforts were not just limited to combat operations. We also provided the World Food convoy commander with “comms-on-the-move.” This capability allowed the convoys to stay in continuous contact with air support and ground command channels in the complex, mountainous terrain, mitigating exposure to attacks—they no longer needed to halt movement to establish communications.

The employment of BACN directly improves joint and combined force operations. It extends ground command and control tactical communications across the region to allow the coalition to task any available air asset to respond to a troops-in-contact situation. BACN also enables the coalition to extend and unify the air picture (to include air track, aircraft orbit and targeting information) for U.S. Air Force, Army, Navy, Marine Corps and British, French and Dutch forces.

Summary

In closing, I would like to thank the Committee for this opportunity to highlight the outstanding efforts of the dedicated men and women of the United States Air Force to secure our Nation in cyberspace. I trust I have illustrated that this new domain is both highly complex and extremely challenging, but it is one that the Air Force is fully embracing. Thank you again and I look forward to your questions.