PERSPECTIVES ON CYBER POWER

CPP-2

Cyber Workforce Retention

William E. Parker IV
Major, USAF

AIR FORCE RESEARCH INSTITUTE PAPERS

Air University

Steven L. Kwast, Lieutenant General, Commander and President

Air Force Research Institute

Dale L. Hayden, PhD, Director

AIR UNIVERSITY

Air Force Research Institute
Perspectives on Cyber Power

Cyber Workforce Retention

William E. Parker IV
Major, USAF

CPP–2

Air University Press
Air Force Research Institute
Maxwell Air Force Base, Alabama

Project Editor
Jeanne K. Shamburger

Copy Editor
Carolyn Burns

Cover Art, Book Design, and Illustrations
Daniel Armstrong

Composition and Prepress Production
Nedra O. Looney

Print Preparation and Distribution
Diane Clark

AIR FORCE RESEARCH INSTITUTE

AIR UNIVERSITY PRESS

Director and Publisher
Dale L. Hayden, PhD

Editor in Chief
Oreste M. Johnson

Managing Editor
Dr. Ernest Allan Rockwell

Design and Production Manager
Cheryl King

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
afri.aupress@us.af.mil

http://aupress.au.af.mil/
http://afri.au.af.mil/

AFRI AU PRESS
AIR FORCE RESEARCH INSTITUTE

Library of Congress Cataloging-in-Publication Data

Names: Parker, William E., IV, 1973- author. | Air University (U.S.). Air Force Research Institute, issuing body.
Title: Cyber workforce retention / William E. Parker IV.
Other titles: Air Force Research Institute perspectives on cyber power ; CPP-2.
Description: Maxwell Air Force Base, Alabama : Air University Press, Air Force Research Institute, 2016. | Series: Perspectives on cyber power,
ISSN 2329-5821 ; CPP-2 | Includes bibliographical references.
Identifiers: LCCN 2016036505 | ISBN 9781585662647
Subjects: LCSH: Cyberspace—Military aspects—United States. | United States. Strategic Command (2002-). Cyber Command. | Information warfare—United States. | United States. Air Force—Recruiting, enlistment, etc. | Airmen—United States.
Classification: LCC U167.5.C92 P37 2016 | DDC 355.3/43—dc23 | SUDOC D 301.26/31:2
LC record available at https://lccn.loc.gov/2016036505

Published by Air University Press in October 2016

Disclaimer

Air Force Research Institute Perspectives on Cyber Power

We live in a world where global efforts to provide access to cyber resources and the battles for control of cyberspace are intensifying. In this series, leading international experts explore key topics on cyber disputes and collaboration. Written by practitioners and renowned scholars who are leaders in their fields, the publications provide original and accessible overviews of subjects about cyber power, conflict, and cooperation.

As a venue for dialogue and study about cyber power and its relationship to national security, military operations, economic policy, and other strategic issues, this series aims to provide essential reading for senior military leaders, professional military education students, and interagency, academic, and private-sector partners. These intellectually rigorous studies draw on a range of contemporary examples and contextualize their subjects within the broader defense and diplomacy landscapes.

These and other Air Force Research Institute studies are available via the AU Press website at http://aupress.au.af.mil/papers.asp. Please submit comments to afri.aupress@us.af.mil.

Contents

Illustrations

Figure

Table

About the Author

Maj William E. Parker IV is the operations officer for the 51st Force Support Squadron, Osan AFB, Republic of Korea, and assists the commander with all personnel and manpower functions that support USAF operations across the Korean peninsula. He has served in various squadron-level base operations support positions leading a combined team of military personnel and civilians managing installation temporary lodging facilities, appropriated and nonappropriated food service facilities, fitness and sports centers, libraries, mortuary affairs services, civilian and military human resources, and squadron contingency programs. He has also held several Pentagon assignments, including chief, Air Force Fitness and Lodging Policy; deputy chief, A1 Issues Team; executive officer, Air Force Directorate of Services; and Air Force Strategic Policy Fellow, US Department of Labor and the Office of the Under Secretary of Defense for Personnel and Readiness. Major Parker has deployed multiple times in support of Operations Iraqi and Enduring Freedom, including as a deployed squadron commander. He holds a bachelor of science degree in public administration, Evangel University, Missouri; a master of science degree in personnel management, Troy University, Alabama; and a master of science degree in international hospitality management from the University of South Carolina.

Preface

I have to admit I chose this topic based on personal curiosity combined with my associated lack of knowledge of cyber warfare and cyber-skilled personnel. This motivation was certainly increased by the current environment. In one news headline, you read of major force reductions the military services are experiencing and predicting under the shadow of the pending return of sequestered budgets in fiscal year 2016. On the following page is a "call to arms" of sorts regarding the need to drastically increase our nation's uniformed cyber-skilled operators. This dichotomy in itself was fascinating, leading me to question the Air Force's ability to retain and grow our cyber forces while simultaneously shedding or stagnating the growth of personnel in almost every other operational community.

I was originally inspired to conduct my study by the Air Force decision in the fall 2014 to establish a distinct cyber operations Air Force specialty code (AFSC) for officers (17S) and to investigate methods and policies to support this new career field's growth and retention. However, once I began to research the expanding cyber mission within the Air Force, I learned that in reality Airmen from several officer and enlisted AFSCs are involved in the Air Force's cyber operations. They include the enlisted 3DX cyberspace support personnel and 1NX intelligence personnel as well as 14N intelligence officers and the 17D/S cyber operations officers who lead and manage Air Force cyber operations. I soon learned that it is the 1B4 enlisted Airman who possesses the highest proficiency of technical cyber skills and on a daily basis is the true "operator, trigger puller" for the Air Force in cyberspace. Further, these Airmen have the cyber skills most desired in both the public and private sectors.

Ultimately, my final motivation in settling on this topic is my strong feeling that the Department of Defense's increased focus, energy, and resources directed toward growing our defensive and offensive operational capabilities in the cyber domain are necessary and justified. The most critical element in supporting this effort is to ensure that we supply human capital that can successfully operationalize this domain.

Acknowledgments

A study such as this one cannot be accomplished without the support of others, and I am overwhelmingly thankful to those individuals who contributed their knowledge and expertise. Most critical to providing the background and context for the evolution of the 1B4s in support of this research was CMSgt John Sanders, career field manager for the 1B4s at the time this paper was drafted. Without his outstanding and supportive cooperation, this project would not have been possible. Other key contributors were Capt Christopher Price and 2d Lt Greg Renner from the US Air Force Directorate of Force Management Policy (AF/A1P); they provided superb support, undergirding my knowledge on the metrics associated with career field health and sustainment. I would also like to thank Mr. Steve Galing and Mr. Bill Dougherty from the Office of the Secretary of Defense's Compensation Policy Office; they provided me with great insights into the historical use of compensation tools to support retention in the Department of Defense. Finally, I would like to recognize Dr. Panayotis Yannakogeorgos, Air Force Cyber College, for his academic advisement and guidance for this project and Ms. Jeanne Shamburger, Air Force Research Institute, for transforming my initial drafts into this comprehensible final product. I thank you all.

Abstract

Experienced cyber and information security professionals will be members of one of the fastest growing and in-demand occupational categories in the labor markets in the United States and around the world in the coming years. This demand is increasing based on the rising threat of cyber incidents, the burgeoning cost of doing business due to cybersecurity infiltrations, and corporate America's / senior executives' growing awareness of and focus on the need to enlarge cybersecurity capabilities in the private sector. The escalating call for cybersecurity professionals collides with a world labor market already experiencing a dramatic deficit in individuals with these skills.

At the same time, the United States Air Force is dramatically increasing the size and capability of its cyber forces to meet its increased contribution to US Cyber Command's (USCYBERCOM) cyber mission forces. The Air Force's enlisted 1B4X Airmen, Cyber Warfare Operations, will be on the leading edge of this contribution to USCYBERCOM. However, this new career field is currently manned at 46 percent, principally due to rapidly increasing requirements. The Air Force specialty code's approximately 210 initial authorizations when it was established in fiscal year (FY) 11 may grow to as many as 880 authorizations by FY 16. This paper's focus is on developing strategic recommendations to effectively retain and sustainably build the Air Force's workforce of 1B4 cyber Airmen, who possess these highly desirable, portable cyber skill sets. Such development will be most critical in the next few years as the Air Force continues to increase its contribution to the nation's cyber mission forces in this new and exciting warfare domain.

This study first overviews the current cybersecurity human capital environment, specifically exploring the increased demand and associated shortage for cybersecurity experts in the marketplace. It then examines the evolution of a new breed of warrior—the Air Force's 1B4 cyber Airmen—and the plan to move this emerging career field from growth to future sustainment. As part of this examination, this study assesses the Air Force's current retention of these highly skilled Airmen. This assessment is followed by a review of contemporary public-sector retention studies and initiative findings, which could prove useful in supporting the retention of cyber Airmen. Also analyzed are Department of Defense retention tools, primarily in the form of special and incentive pays, to determine their effectiveness in supporting retention within the armed forces and their potential application in supporting cyber Airmen retention as measured by recent research and studies. Finally, this study summarizes recommended initiatives and focus areas to support not only retention of cyber Airmen but also growth and sustainability of this fledgling career field.

Chapter 1

Rising Demand for Private-Sector Cyber Skills

> *Growth in demand* [for cyber personnel] *continues to far outnumber the personnel capable of protecting our networks.*
>
> —Cong. Jim Langevin (D-RI)

Experienced cyber and information security professions will be one of the fastest developing and in-demand occupational categories in the United States and around the world in the coming years. Recent, highly publicized criminal-underworld hacking incidents directed against recognizable and trusted companies in the private sector include Target Corporation, the Home Depot, J. P. Morgan, and Sony Pictures Entertainment. These occurrences have only highlighted the increased threat to our nation in cyberspace and fueled the fire in private-sector demand for those with cybersecurity expertise. Perpetrators can be single, reclusive attackers who attempt to penetrate networks from the comforts of home. They can also belong to large, well-funded, organized criminal rings with deep pockets; a host of computing resources; and professional, trained hackers at their disposal. Other threats continue to emerge from unseen state-sponsored assailants who blur the lines between criminal intent and acts of national aggression—witness the Sony hacking incident in late 2014. While the motivations and resources available to potential attackers in the cyber sphere are diverse and warrant different national responses, the rising and varied threats in cyberspace have led the public and private sectors to become more aware of their vulnerability in that realm. This realization has led to a rapidly growing demand for cyber-skilled defenders—who are increasingly in short supply.

For the United States Air Force, enlisted 1B4 cyber-warfare operations Airmen are on the leading edge of cyber defensive and offensive operations. The present demand for cybersecurity specialists in both the public and private sectors could undoubtedly lead the Air Force to be significantly challenged in retaining its most developed and experienced cyber Airmen in the years ahead. Airmen in several officer and enlisted Air Force specialty codes (AFSC) are involved in Air Force cyber operations, including enlisted 3DX cyberspace

---

Major Parker wrote this paper in June 2015 as an Air Force Fellow.

support personnel, 1NX enlisted intelligence personnel, 14N intelligence officers, and 17D/S cyber operations officers who lead and manage Air Force cyber operations. It is the 1B4 Airmen, however, who possess the highest level of technical cyber proficiency and on a daily basis are the true "operators, trigger pullers" in cyberspace. They have the cyber experience most desired in both the public and private labor-market sectors. Consequently, this paper focuses on developing a strategy to effectively retain and sustainably build the Air Force's workforce of 1B4 cyber Airmen with these highly desirable, portable cyber skill sets. Doing so will be most critical in the next few years as the Air Force continues to increase its contribution to the nation's cyber mission forces in this new and exciting warfare domain.

We are experiencing what the Center for Strategic and International Studies (CSIS) and many others have described as a "human capital crisis" in the cybersecurity workforce, where demand continues to outpace supply. It is estimated that today 30,000 unfilled cybersecurity jobs exist in the US federal government sector alone.[1] According to the International Information System Security Certification Consortium (ISC), the US public and private demand will increase 11 percent per year over the next few years.[2] Some estimates have placed the worldwide public and private workforce shortage for cybersecurity professionals at close to one million and counting.[3] However, it is worth noting that these shortages are somewhat ill defined in that "cyber skilled" personnel tend to be grouped into a singularly defined category of "cyber skills." In reality, the skill set is varied and can range from supporting local informational technology, engineering infrastructure, and conducting data analytics to writing cyber code or hacking. The latter is often the most difficult skill set for human resource professionals to identify within the labor pool and recruit.[4] In the current environment, shortages in all flavors of cyber experts will increase, at least in the foreseeable future. Demand for all varieties of cybersecurity-skilled experts in both the private and public sectors is only rising.

What is driving this increased demand? Without question, recent hacking events that have continued to play out in the daily news and have grabbed American and world headlines only fuel it. Each of these events has been increasingly damaging, cumulatively draining the targeted organizations of millions of dollars in stolen or unrealized revenues, exposing millions of their customers to identity theft and fraud, and, in the case of Sony, threatening constitutional liberties. Few people understand that these major and widely publicized hacking events barely scratch the surface of the current and emerging cyber threat.

Part of the problem is that cyber events spring from myriad sources with equally diverse motivations, spanning individual hacktivists and criminals,

terrorists, organized crime, and state actors—including foreign-sponsored intelligence or military organizations. While these players differ in their motivations and capabilities to perform nefarious acts in cyberspace using a diverse and ever-growing list of cyber weapons, more importantly, the trend of major cyber events is only worsening—capturing national interest. Since 2006 the CSIS has maintained a listing of major cyber events, which it defined as any successful attack against a government or company resulting in a significant loss of data or a million dollars or more. From May 2006 through 15 December 2014, it recorded 172 major cyber incidents. One case in 2012 indicated that the Chinese had accessed classified information regarding vulnerabilities of the F-35 Joint Strike Fighter—the most costly weapon-system investment in US history. Another was a criminal hacking scheme in Oman and the United Arab Emirates in 2013 involving eight individuals who stole more than $45 million. The listing includes 66 reported events in the first four years from the list's creation in May 2006 to May 2010, followed by 88 events in the following four years by the end of May 2014. Unfortunately, the upward trend in major events has only continued from June through December 2014, when 18 additional major events were reported on the list in seven short months.[5] Clearly evidenced in a review of this incident list is the steady rise of the frequency and boldness of major cyber incidents. Moreover, the costs are escalating for each incident not only in terms of direct and immediate financial loss but also in prestige and public confidence for those companies involved, ultimately leading to further fiscal damage.

Cybercrime is now estimated to suck at least $400 billion from the global economy. This staggering figure is more than the gross domestic product (GDP) of many nations' economies, and it is estimated that these losses will only increase in future years.[6] This stunning statistic would lead most organizations in today's global economy to act to increase their cybersecurity. However, many of them have maintained an unwarranted level of self-security in cyber, naively believing they were immune to such damaging losses. While the recent highly publicized hacking events certainly started to heighten the focus on cybersecurity at home and abroad, the associated financial losses from cyber incidents are the true motivator driving organizations to action. In a 2014 survey of 500 domestic private and public organizations, more than 7 percent reported losses of $1 million or more in the last year, and 19 percent reported losses between $50,000 and $1 million in cybercrime-related incidents.[7] This representative sample within the United States suggests that more than a quarter of all US businesses may expect a significant cybercrime within the next year, and it is now estimated that the US economy is losing 0.64 percent of domestic GDP to cybercrimes.[8] Speaking more directly to the increased

cost per cyber incident, a Ponemon Institute report following another 2014 study stated that the average annual cost for each company victimized by cybercrimes was $7.6 million of direct, indirect, or opportunity costs—a 10.4 percent increase from the previous year. The survey also found that companies investing in cybersecurity defenses saved substantially more than those that did not, with an average 15 percent return on investment (ROI) if seven core cybersecurity initiatives are implemented. At the top of the list in terms of ROI savings initiatives was employing adequate cybersecurity personnel, with an average ROI of $1.3 million.[9] The collective effect of these reports—each describing the growing threat in cyberspace and the overwhelming figures in terms of lost revenues related to cyber incidents—has been to grab the attention of executives across the nation. It is motivating them to increase their organizations' cybersecurity capabilities, starting with the acquisition of skilled cybersecurity experts.

A malicious cyber event bringing the issue of cybersecurity to the forefront of every CEO in America and simultaneously increasing the stock value of cybersecurity specialists came after Target's breach in late 2013, according to Joe Hernandez, J. P. Morgan's executive director and global head of cybersecurity strategy and architecture.[10] Target's well-publicized incident, which unmasked 40 million customer credit cards to hackers, eventually led to the sacking of 35-year Target employee and CEO Greg Steinhafel. The overall value of Target's stock fell more than 30 percent in a few short months following the breach.[11] This was the first time a cyber intrusion led to the firing of a major domestic company executive, causing a huge ripple effect within corporate America, according to Hernandez. This shockwave led to a new prominence for cybersecurity, placing the establishment of effective organizational cybersecurity right behind company liquidity as the top two priorities for many organizations.[12]

Hernandez stated that the most influential factor in this change in priority was tying cybersecurity performance to pay for executives within all divisions of the organization, an action that he believes led to a "laser focus" from executives on cyber issues. CEOs are thus incentivized to be directly involved in cybersecurity efforts, leading to multiple cyber ramp-up initiatives. In the case of J. P. Morgan, this emphasis translated to a host of actions. These included an explosion in the cybersecurity budget from $250 million in 2014 to $420 million in 2015, weekly executive-level meetings with cybersecurity experts, the installment of chief information officer positions at the top of each division within J. P. Morgan, and the establishment of three global cybersecurity operations centers: New York City, London, and Singapore—all opened in 2014. Martinez said that J. P. Morgan's reaction is certainly indicative of a

larger movement to focus on cybersecurity in the private sector. The company has shared intelligence and resources on cyber threats, even going as far as establishing partnerships with market competitors to bolster cyber defenses. Such defenses are not a point of competitive advantage but are based on a collective exposure in the marketplace.[13]

However, Hernandez clearly identified the Achilles' heel in J. P. Morgan's and the private sector's cyber ramp-up initiative: the shortage of cyber professionals in the labor pool. He attributes this deficit to stiffened competition to recruit skilled personnel, in turn enabling such recruits to negotiate higher wages. Fortunately, he said, J. P. Morgan is committed to offering competitive compensation packages not only to improve its chances of drawing more cyber experts from this pool but also to retain those it has today.[14]

Clearly, the value of cybersecurity experts continues to swell in a labor market already experiencing a deficit. Driving this phenomenon are the increased frequency of major cyber incidents, the rising costs per incident, and a new focus from company executives on increasing cybersecurity capabilities. So why is it that the labor market continues to fall so short of demand?

The answer to this question is really very simple: a production problem. First, a drastic reduction has occurred in the number of students following education tracks in the computer sciences since the dot-com crash in the early 2000s. The United States peaked with 60,000 students completing computer science degrees in 2004—the last group of graduates who entered the education system prior to the dot-com crash—but experienced a reduction to an average of about 38,000 graduates per year since 2008, a 37 percent annual decrease.[15] Another alarming trend has been the decrease of females pursuing computer sciences over the past decade from 23 percent of all computer science degrees awarded in 2004 to 18 percent in 2014, a period in which physical and hard science degrees increased only slightly across the nation.[16]

The shortfall of cybersecurity experts and reductions in the associated training pipeline were identified several years ago in the 2010 CSIS report *A Human Capital Crisis in Cybersecurity*, produced by the Commission on Cybersecurity for the 44th Presidency (President Obama). It concluded that "a critical element of a robust cybersecurity strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where we are weakest."[17] This report listed strategic recommendations to grow the capacity of cyber-skilled professionals in the domestic workforce and included key initiatives shared among the federal government, academia, and industry. These efforts to date have supported increasing educational opportunities for cyber-related studies, with more than 100 colleges now offering information assurance programs supported by

the National Security Agency (NSA) and 40-plus states identified as Centers for Academic Excellence schools.[18] At the same time, the NSA has endorsed 12 public and private university cyber-surety programs nationwide whose curricula it has certified.[19]

Unfortunately, the production of these schools has yet to meet demand, leaving organizations to seek alternative means to satisfy their needs. That is, many organizations have chosen to recruit and build cybersecurity talent internal to the organization and have implemented rigorous training plans for employees identified with aptitude for cybersecurity operations.[20] Despite these production efforts, a recent RAND study on the cybersecurity labor market corroborates that a serious shortage persists today. However, the study asserts that current efforts in the labor market, education, industry, and government—coupled with anticipated improvements in technology and computer architecture—will create an equilibrium between labor demand and supply for cybersecurity professionals in the longer term, possibly within 10 years. Thus, additional steps to deepen the pool for most cybersecurity professionals may be unnecessary (although highly skilled experts will remain in demand).[21]

Of course, the final option for increasing the number of cyber professionals for organizations will be to attract, recruit, and hire experienced, cyber-skilled personnel from the existing pool. In fact, human resources experts indicate that the best predictor of an individual's ability to effectively perform cybersecurity position requirements is previously demonstrated experience and competency in cyber operations—not personally obtained certifications or educational background—leaving this option as a somewhat risky endeavor.[22]

The Air Force must note from these environmental factors not only that the nation is experiencing a major deficit in the labor market in cyber skills but also that options for increasing organizational capacity for cyber professionals are limited. Organizations may hire directly from educational programs, an action that is not meeting growth demands; develop their own cyber-skilled personnel; or draw from the limited cyber talent pool. Thus, cyber Airmen—particularly experienced 1B4s—will be directly in the crosshairs of the growing number of organizations seeking to increase cybersecurity capabilities in both the public and private sectors, potentially drawing these personnel away with more lucrative offers. Regardless of the long-term labor market predictions for cybersecurity, today's significant shortage of cybersecurity specialists will last at least through the foreseeable future. This shortage will continue during a period when the Air Force is expected to increase its cyber workforce and capabilities. With that prospect in mind, the Air Force must seek to integrate effective personnel and other policies now. Doing so will support

the retention and sustainability of a healthy cyber mission force for both the short and long term.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Summers, "Raising a Cyber Army"; and Asch et al., *Cash Incentives*.
2. Fung, "You Call This an Army?"
3. CISCO, *Annual Report 2014*, 60.
4. Kay, Pudas, and Young, "Preparing the Pipeline," 2–6.
5. "Significant Cyber Incidents."
6. Center for Strategic and International Studies (CSIS) and McAfee, *Net Losses*, 2.
7. Mickelberg, Pollard, and Schive, *US Cybercrime*, 5.
8. CSIS and McAfee, *Net Losses*, 9.
9. Ponemon Institute, *2014 Global Report*, 1, 3–4, 21.
10. Hernandez, in discussion with the author, J. P. Morgan, New York, 11 February 2015.
11. Leonard, "Cybersecurity Professionals in Demand."
12. Hernandez, discussion.
13. Ibid.
14. Ibid.
15. Fung, "You Call This an Army?"
16. Korn, "Number of College Students."
17. Evans and Reeder, *Human Capital Crisis*, v.
18. Fung, "You Call This an Army?"
19. Yannakogeorgos, outbrief, slide 14.
20. Kay, Pudas, and Young, "Preparing the Pipeline."
21. Libicki, Senty, and Pollak, *H4CKER5 WANTED*, 71–77.
22. Kay, Pudas, and Young, "Preparing the Pipeline."

Chapter 2

Air Force Cyber Warfare Operations (1B4X)

Cyberspace will only grow as the recognized domain through which critical information must flow at ever-increasing volume and speed. As the global community increases its dependence on access to these commons and freedom within them, their vulnerabilities will invite actions with potentially disastrous worldwide consequences. Accordingly, the demand for ensuring confidence in the integrity of these commons will increase in the years ahead.

—*America's Air Force: A Call to the Future* (July 2014)

Cyber warfare is fought on a battlefield like no other. It is an unseen battlefield that cannot be felt or smelled, a place where the battle cannot be witnessed by thousands of warriors simultaneously or by the common man as have other battles since the beginning of time. However, the threat and effects of this new form of warfare have proven tangible, driving senior military leaders to develop both defensive and offensive capabilities within the domain. Early on, people realized that this new domain of warfare would require a different kind of warrior. Success on this battlefield would hinge not as greatly on fielding and employing a dominant weapon system, as in more recent conflicts, but on the individual skills and abilities of the warriors operating in this unique domain.

Evolution of Air Force Cyber Warriors

Operating on the front lines of the cyber domain are the Air Force's 1B4s or cyber warfare operations enlisted personnel. This distinct career field was created in late calendar year 2010, beginning with the immediate conversion of about 200 cadre Airmen filling cyber offensive and defensive mission units and positions. The 1B4 AFSC is relatively new, but more than 10 years earlier, Airmen filled similar roles in hyperclassified network warfare squadrons under special duty assignments. Most were legacy 3CO Airmen from the former communications career fields who later returned to their career fields following completion of their special duty assignment. However, even before then, in the 1980s and into the 90s, the Air Force led the way for cyber warfare for the Department of the Defense (DOD). This mission took place behind closed doors and out of the public eye; sadly, much of that early pioneering cyber

heritage has been lost.[1] This loss of heritage has resulted in a forfeiture of opportunity to build community identity for cyber Airmen as well as to capture early cyber doctrinal foundations much needed as the force expands.

As the Air Force established Air Force Cyber Command and the Twenty-Fourth Air Force became operational, greatly increasing the number of Airmen within the cyber ranks, it became evident that the service needed to establish a stand-alone cyber defensive and offensive career field to build the level of depth and expertise for operating effectively on the cyber battlefield. When 1B4 was established, initial predictions were for the AFSC to grow to 350 authorizations over five to six years. However, much has changed since then, and the career field is now expected to grow to about 880 authorizations by fiscal year (FY) 16. This rapid acceleration has been simultaneously and directly linked to the expansion and maturation of the United States Cyber Command (USCYBERCOM) mission. Notably, the command doubled its budget in 2014 to $447 million and in recent years announced it would triple the size of its operational forces—even though the remainder of the DOD continues to hemorrhage under the shadow of the return of sequestered budgets in FY 16.[2] As part of this growth, USCYBERCOM tasked the Air Force to have 1,715 Airmen in joint cyber mission force teams by FY 16, many of whom will be 1B4 personnel. Thus, while much of the rest of the Air Force was trimming the size of its force in recent years—most notably in FY 14 during the last round of major force-management programs—1B4 authorizations have grown in rapid succession each year since FY 11. As would be expected with such drastic growth in a highly technical field that was and continues to be a cross-train-only AFSC, manning levels have struggled to keep pace with the rise in authorizations (tables 1 and 2). The 1B4 manning currently sits at just 46 percent, and the career field is struggling to dig out of an ever-deepening hole as additional authorizations have been added each FY since its inception.

Table 1. 1B4X manning (excluding students/transients/prisoners) end of (EO) FY 2011–February 2015

	Sept. 2011	*Sept. 2012*	*Sept. 2013*	*Sept. 2014*	*Feb. 2015*
Authorizations	268	371	412	545	759
Inventory	240	260	303	341	354
Manning percent	89%	**70%**	**73%**	**62%**	**46%**

Provided by CMSgt John Sanders, 1B4X CFM, Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO) A6/A6SF, 15 March 2015.

Table 2. Zone manning EO FY 2011–February 2015

	Sept. 2011	*Sept. 2012*	*Sept. 2013*	*Sept. 2014*	*Feb. 2015*
Zone A	208%	167%	97%	163%	128%
Zone B	81%	86%	70%	91%	71%
Zone C	90%	70%	51%	52%	34%
Zone E	44%	38%	32%	30%	24%

Provided by CMSgt John Sanders, 1B4X CFM, SAF/CIO A6/A6SF, 15 March 2015.

Accessions

Cross-train accessions for 1B4s—a retrain-only AFSC—are accepted from personnel having any AFSC, but applications are stringent and competitive. Time-in-service (TIS) requirements for retraining are currently broad; retraining is open to those between 4 and 14 years of service (YOS) in grades from senior Airman to master sergeant. However, candidates will be considered only if they have scored a minimum of 64 in the general category on the Armed Services Vocational Aptitude Battery (ASVAB) and a minimum of 60 on the electronic data processing test. Additionally, retrain request packages must include the member's last three enlisted performance reports and may include an optional letter of recommendation to the enlisted career field manager (CFM). The 1B4 CFM makes the final selections of retraining candidates only after an individual interview with the candidates and after they have completed a 40-question skills assessment.[3] Although this long and demanding selection process enables the CFM to choose from the "best of the best" in the Air Force, it does slow down the overall time from application to selection and the process of finally producing a mission-ready cyber Airman.

Under the shadow of such a large deficit in manning levels, the career field is currently programmed to bring in 150 cross-trained personnel yearly for the next few fiscal years. However, both the 1B4 CFM and the chief of cyberspace training for Air Force Space Command believe that meeting the growing demand in 1B4s may call for increasing this number anywhere from 210 to 300 annual slots to satisfy the bow wave requirement of increasing annual 1B4 authorizations. Before such an increase can be absorbed, the Air Force realizes that logistical impediments in classrooms, equipment, and instructors must be sorted out. It is confident, however, that it may soon overcome these shortfalls, enabling more accessions by FY 17.[4]

Training

Once selected for retraining, Airmen must complete roughly 105 days of combined prerequisite certifications and Cyber Operations Apprentice initial skills training (IST) at Barksdale AFB, Louisiana, for award of the 3-level certification as a 1B4. Immediately after IST, trainees begin more specific mission/position training under the initial qualification training (IQT) block, which ranges from one to four months depending on the track and weapon system. Subsequently, Airmen report to their units for weapon system training specific to the unit's mission. A mission certification period follows that also varies in length; it validates that the Airman is mission ready and available for crew duties.

All told, the process ranges from 8 to 14 months from the start of IST until an Airman meets minimum mission capability levels at the operational unit. This time does not consider the additional period needed to build experience to reach full combat proficiency. Also worth noting is that about 20 percent of Airmen selected to cross train are eliminated at some point in this process for failure to master the complexity of the training material. The cost involved in the full training process is high. The estimated average training cost, which includes the trainee's salary for just the initial IST period, is $65,000 per newly minted cyber warrior (including approximate student wages). This amount does not include the expense for IQT and unit-level mission training. One would expect that such a long and costly training pipeline, which also adds to an Airman's resume a highly technical and portable skill set for the civil sector, would incur a lengthy active duty service commitment (ADSC). However, the ADSC for those who complete IST is three years, a commitment that the Air Force must examine to influence retention of 1B4s. Figures 1 and 2 depict the training progression for the cyber defense career field.

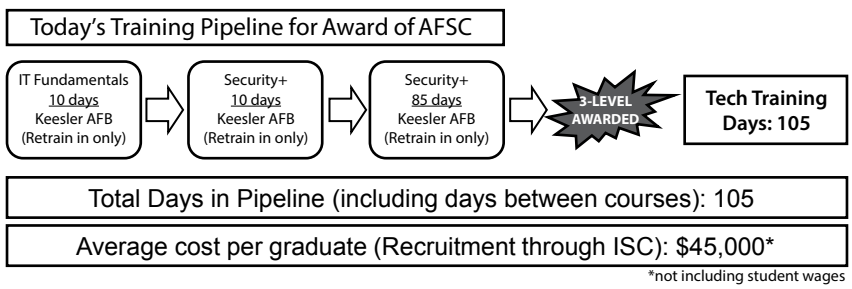
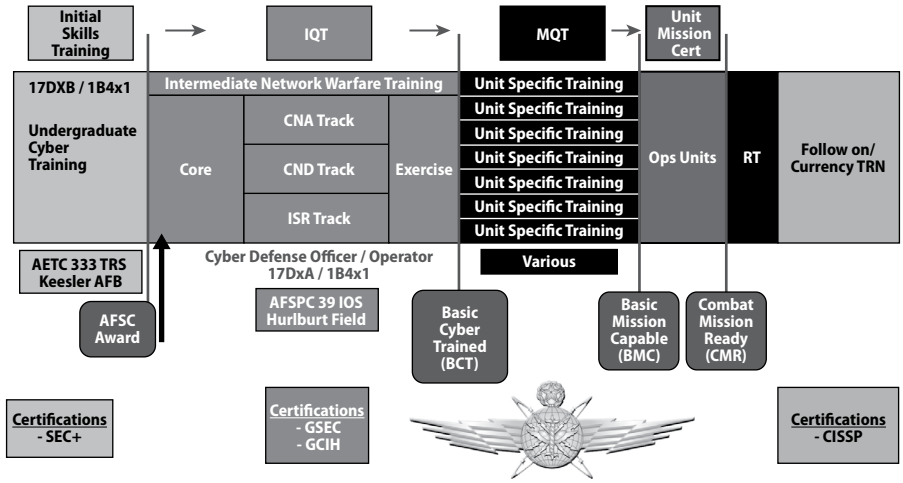


Figure 1. Training pipeline for award of cyber AFSC. (Provided by CMSgt John Sanders, Secretary of the Air Force, Office of Information Dominance and Chief Information Officer [SAF/CIO] A6/A6SF, 15 March 2015.)



CISSP Certified Information Systems Security Professional
CNA Computer network attack
CND Computer network defense
GCIH GIAC Certified Incident Handler
GSEC Global Information Assurance Certification (GIAC) Security Essentials
RT Refresher training
SEC+ Security+

Figure 2. Cyber operator cyber mission resilience road map. (Provided by CMSgt John Sanders, SAF/CIO A6/A6SF, 15 March 2015.)

Airmen entering the retrain-only 1B4 career field are typically older and more educated compared to most personnel who initially enter a career field. In the last FY, the average TIS for retrain accessions was about 6 years upon selection for retraining, putting most Airmen at 7 to 7.5 years TIS once they arrive at their units ready to contribute to the mission. More than 47 percent of 1B4s have earned an associate's degree—double the Air Force enlisted average of 23.6 percent. Another 17.6 percent have completed bachelor's degrees (also double the Air Force average of 8 percent), and 3.6 percent have completed master's degrees (the Air Force average is less than1 percent) although these degrees may not have any application in the cyber arena. The median grade is E-5 (technical sergeant), 71.7 percent are married (54.8 percent is the Air Force enlisted average), and 62.3 percent live with dependents in the household (43.3 percent is the Air Force average).[5] The service must also consider demographic background since it could influence the growth and retention behaviors of the career field.[6]

Career Field Health

A key informational tool provided to CFMs to assess the overall status of any given specialty is the career field health (CFH) chart, produced monthly by the Air Force Directorate of Force Management Policy (AF/A1P). This is particularly true for new and emerging career fields looking to develop long-term sustainability. Figure 3 shows the inventory of 1B4 Airmen by YOSs (not including student and prisoner populations) as of February 2015. The important feature of this chart is the red sustainment line, which is the measure of health as it relates to personnel available within the career field by YOS. A1PF calculates sustainment lines, with the major influencers of the size and shape of the curve being the total authorizations from the unit manning document UMD (reflected in height of the curve) and the historical retention and accession behaviors of the career field (reflected in shape of the curve). The CFH chart indicates that 1B4s fall well below the sustainment line for nearly every YOS, indicative of the field's 46 percent manning. Much of this shortfall is of course somewhat artificially created by the rapidly increasing authorizations since the career field's inception. Another peculiarity of the curve's shape is that the sustainment line does not start until three YOSs and increases all the way through 17 to 18 YOSs before it plummets at around year 20. This decline is largely due to the current cross-train accessions policy for the career field allowing crossflow up to 14 YOSs. The sustainment line visibly differs from that of a more traditional field using initial accessions—indicative of the majority of the force as illustrated by the total Air Force enlisted chart (fig. 4).[7]

Obviously, filling the gaps that extend all the way through the sustainment line makes retaining Airmen of utmost importance as the career field matures. This infant career field is in a period of rapid expansion and on the cutting edge of building joint cyberspace capabilities. Thus, this study must expand its scope beyond offering recommendations for retention strategies to encompass those for healthy force sustainment throughout the entire life cycle, from initial entry to the end of sustainment requirements.

Understanding that the desire is to influence 1B4 sustainability holistically along the entire life cycle, one should note that sustainment lines are not static. Many factors influence changes in the shape of these lines. One example is accessions policy, as indicated above regarding the current retrain policy. As authorizations have increased each year and gaps have continued to grow in meeting sustainment through 23 YOSs, it has made sense to offer cross-

training opportunities for 1B4s through 14 YOSs to help fill the gaps as far out in the life cycle as possible. However, to engender long-term stability and sustainability in the career field, the enlisted CFM for the 1B4s desires to implement other solutions as well. As authorization numbers stabilize and manning increases to reach sustainability, he wants to begin introducing initial accessions into the manning equation. By installing Airmen earlier in the career life cycle as 1B4s, the Air Force can begin to increase the depth of experience. Over time this change in policy would most certainly affect the sustainment line shape, shifting it toward a more traditional one by potentially extending the average career length and building a more experience forced of 1B4s. To achieve this normalization, the Air Force must adjust retention plans to account for the potential shift in sustainment. The CFM's plan calls for starting small by introducing about 30 initial-accessions Airmen directly from Basic Military Training in FY 17, counterbalanced by about 130 cross-trainees, as a small but incremental move toward this transition. The eventual goal is to move toward almost all initial accessions for the 1B4s in the long term.[8]

Factors that could hamper this effort include policy and logistics for supporting IST requirements of new accessions at the schoolhouse at Keesler AFB, Mississippi. However, an even larger issue is one presented by USCYBERCOM and cyber commanders desiring "more seasoned" and "mature" cyber operators. In opposition to fulfilling the goal of increasing initial-accessions Airmen into Air Force cyber units, USCYBERCOM has dictated elevated minimum grade levels for operational manning requirements for units. Doing so leaves no positions in which to place initial accessions to grow and mature. The Air Force has acknowledged that many of the more mature cross-trainees in reality may be trained and experienced to only a 3-level as a new 1B4 cyber operator. Nevertheless, their overall maturity in the Air Force is believed to fill the gaps in experience and expertise that a new accession just out of high school would lack. Although introducing new accession 1B4s has its challenges, an alternative used for other AFSCs is a hybrid accessions model that blends new accessions with cross-training. Such a model strikes a balance between enabling the long-term development and utilization of initial accessions Airmen while also injecting more mature and experienced Airmen. This accessions model also offers a more familiar traditional shape to the sustainment line, which could support longer-term retention.

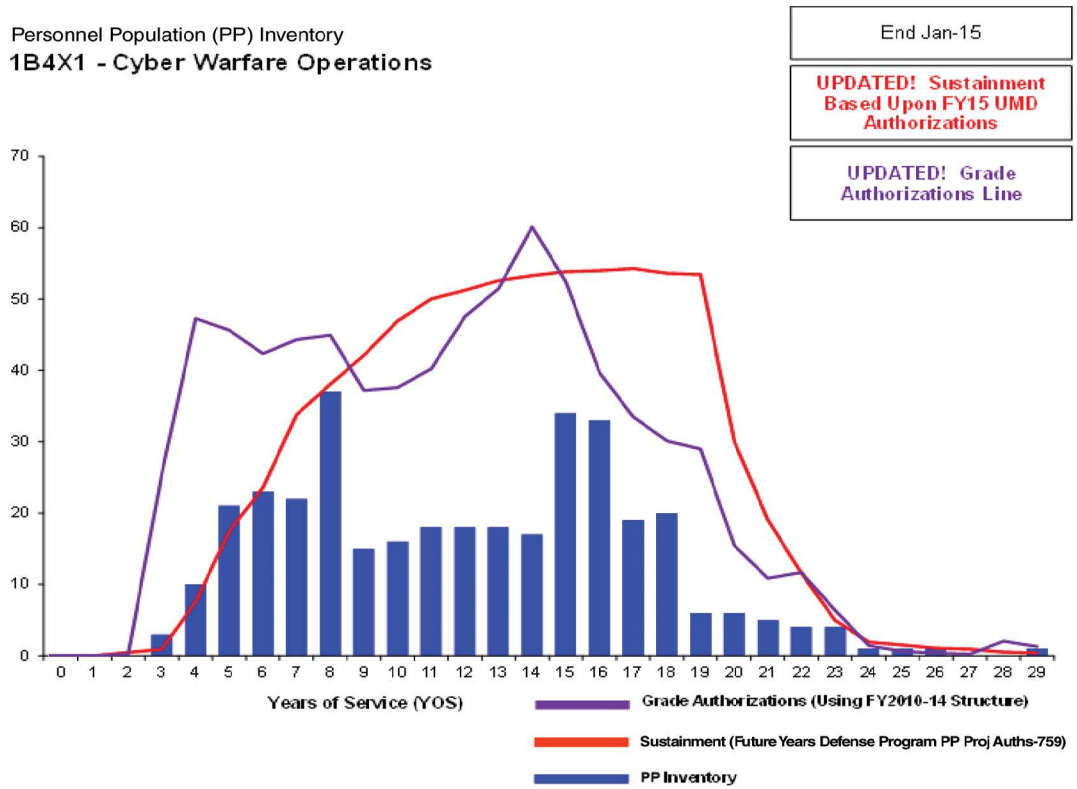


Figure 3. Inventory of 1B4 Airmen by YOSs. (Provided by Headquarters USAF/Deputy Chief of Staff, Personnel; Directorate of Force Management Policy; Force Management Division [HQ USAF/A1PF].)

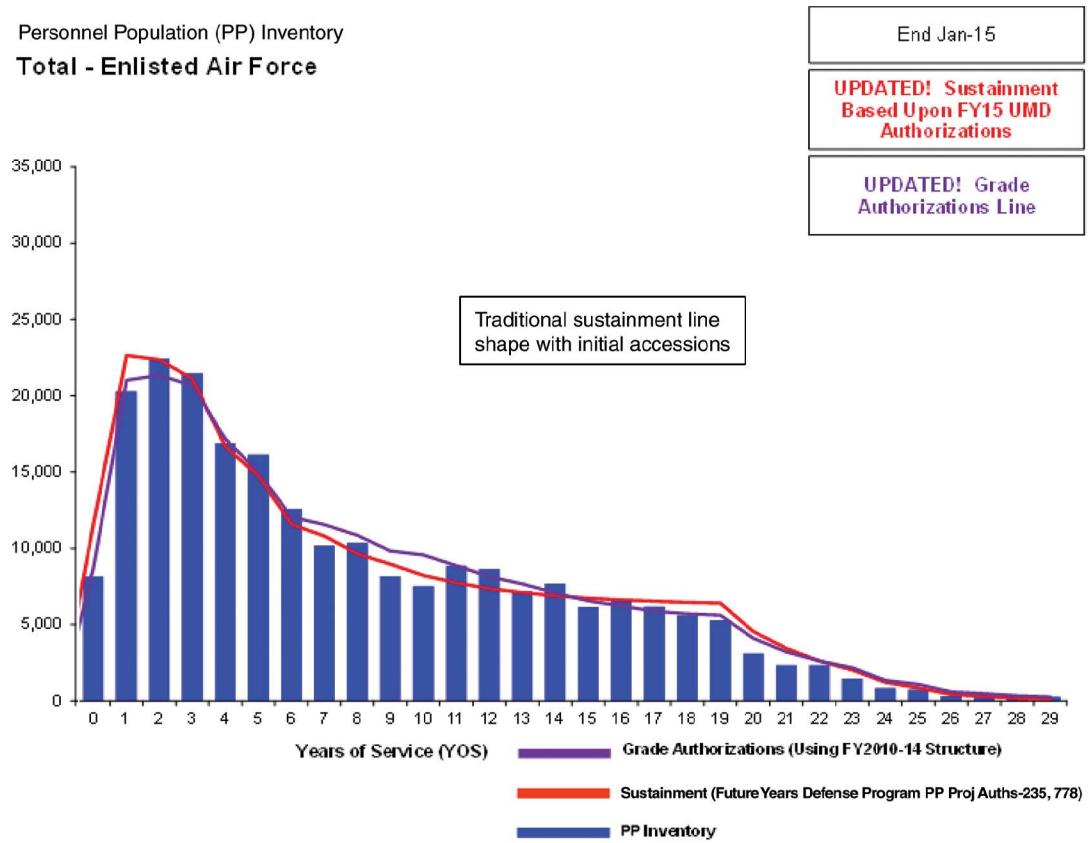


Figure 4. Inventory of total enlisted Air Force by YOSs. (Provided by HQ USAF/A1PF.)

Career Field Challenges

One of the primary challenges for this nascent career field will be managing the production and placement of newly trained personnel to meet the explosion of 1B4 authorizations in units with new or rapidly expanding missions. Another will be defining and communicating the 1B4 career field progression and career path to constituents. Although a notional career pyramid has been produced for the field, the progression path is expected to evolve with changes in missions and roles of 1B4s as the career field continues to expand. Having constant situational awareness of these changes will be critical to ensure that training is properly aligned to mission. It is also essential to ensure that a 1B4 mission/role expectation disconnect does not exist or persist between senior 1B4s and the CFMs and those in the field. Such disconnects can lead to disgruntled Airmen and increased retention issues.

Monitoring retention will be another aspect of gauging career field health, particularly for a relatively small but growing career field in which Airmen coming into the system are gaining technical skills highly desired in the civil sector and in short supply in the labor market. One mechanism for following retention is the monthly CFH charts that track retention trends for the past 16 months in relation to AF/A1PF benchmark goals. These retention benchmark goals are not a measure of the raw number of Airmen the Air Force desires to retain. Rather, they are an algorithm sensitive to the career field's overall environmental circumstances and sustainment goals. In the case of 1B4s, the algorithm must recognize and factor in the need to grow the ranks due to a rapid increase in authorizations and the fact that retrain accessions may be entering the career field through 14 YOSs. It must further consider, among other factors not listed here, "retention boundaries" that take into account the reality of historical retention behavior indicating that losses inevitably occur naturally over time.

Given the 1B4 current circumstance of growing authorizations and low manning as well as the factors just described, retention goals must be set high. As depicted in table 3, they are currently at 87 percent for Zone B (6 to fewer than 10 YOSs), 97 percent for Zone C (10 to fewer than 14 YOSs), and 80 percent for Zone E (more than 20 YOSs). Zone A is a nonfactor since almost everyone is in Zone B for 1B4s; Zone D is rarely monitored since almost everyone over 15 YOSs stays until retirement. For each of these zones, 1B4s failed to meet retention goals in both the monthly measure and the 16-month rolling average. However, a comparison of the retention rate of 1B4s with that of the Air Force average on the CFH chart indicates that 1B4s do not necessarily attrite at a higher rate than does the rest of the Air Force. The high retention

bar stems from the Air Force's need to keep more 1B4s to reach manning targets given current shortages and planned expansion of 1B4s.

Table 3. Retention trends and goals September 2012–February 2015

Zone	*FY 15 goal*	*16-month trend as of Feb. 2015*	*16-month trend EO FY 2014*	*Sept. 2013 snapshot*	*Sept. 2012 snapshot*
Zone A	*.26*	*.84*	*.94*	*.80*	*.90*
Zone B	*.87*	*.67*	*.86*	*.56*	*.79*
Zone C	*.97*	*.76*	*.88*	*.83*	*.68*
Zone D	*.80*	*.64*	*.91*	*.79*	*.77*

Provided by Headquarters USAF/Deputy Chief of Staff, Personnel; Directorate of Force Management Policy; Force Management Division (HQ USAF/A1PF).

To support reaching this goal, the Air Force has offered a relatively conservative selective reenlistment bonus (SRB), with multipliers of two for Zone A, four for Zone B, and three for Zone C. Take rates for the SRB essentially mirror retention trends for each zone, and if Airmen opt to not accept the SRB, they must either separate or retrain. 1B4s were offered the same SRB multipliers by each zone in FY 14—a large increase from FY 13 when only Zone B received a multiplier of one—and no SRB was offered in FY 12.

Overall retention losses may not be high, as indicated by the 16-month trend from the end of FY 2014 to February 2015, but it is worth noting that the rolling retention rate is decreasing. Since little historical data exists for 1B4 retention behaviors, however, one must be cautious not to induce too much from this data. Another proven method for identifying retention trends is by charting the cumulative continuation rates (CCR) over time, which measures the overall tendency for Airmen to stay in service from one year to the next. The chart on the following page, which measures CCRs for 1B4s, identifies retention decision points where the line steepens in descent (fig. 5). The desire is to smooth out this line where it steadily progresses downward through the sustainment life cycle.

As the chart depicts, the steepest declining points are at around year 13 and most notably in year 20. This data reflects that retention decision points are most shaped for 1B4 Airmen at about 12–13 YOSs, or at about five to six years after they've entered the career field (Zone B). This conclusion presumes that the average YOSs for those who have cross-trained and completed training is from seven to eight. For those Airmen who continue service beyond this decision point, many stay until retirement eligibility at 20 YOSs. The most influential

retention decision point is here, with the majority of personnel leaving service at 20 YOSs. This trend is not atypical as many Airmen tend to leave service upon reaching retirement eligibility. However, at present only five 7-level 1B4 Airmen currently on active service with 20 or more YOSs do not have an approved retirement date.

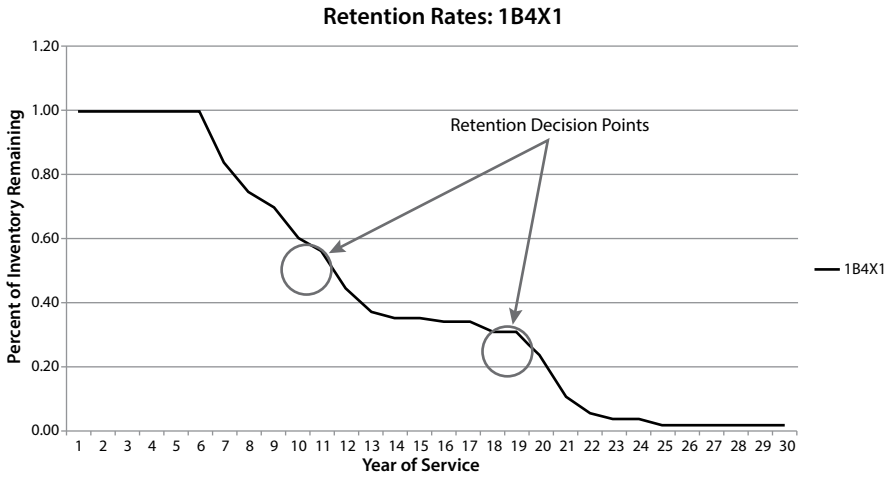


Figure 5. 1B4X1 retention decision points. (Provided by Headquarters USAF/Deputy Chief of Staff, Personnel; Directorate of Force Management Policy; Force Management Division [HQ USAF/A1PF].)

What may be driving this tendency is largely conjecture, but several cyber Airmen gave an idea of underlying reasons: little hope of future promotion and the lure of high-paying civilian employment.[9] Some of this lack of opportunity stems from the limited availability of positions to grow into. Only 14 9-level positions were open to 1B4s in FY 15—albeit a 100 percent increase from 7 such positions in FY 14. Regardless, Airmen who are not upwardly mobile into the highest-level positions but who are highly experienced cyber warriors will be invaluable as they move toward stabilizing and sustaining the Air Force's cyber forces. The 1B4 CFM also noted a disturbing retention trend last FY when he attempted to fill needed vacancies at the schoolhouse at Keesler AFB in support of growing the career field. When assignments were posted for five staff sergeants for instructor duty, each chose to separate rather than move.[10]

The fact that current 1B4 retention levels, although not meeting career-field-specific benchmark targets, are still in line with overall Air Force reten-

tion rates may be somewhat comforting. However, the reality of the growing demand for cybersecurity skilled personnel in the global labor market has motivated the 1B4 CFM to monitor retention and the factors that may drive separation. In a recent occupational analysis survey, the CFM added a voluntary retention question asking respondents in the career field whether they planned to reenlist. This question also offered an option of selecting 31 factors that would most influence their retention decision, with an additional option of providing comments along with the response.

Of the 192 respondents to the base question (intention to stay or go), 160 stated that they planned to reenlist while 32 indicated that they would separate.[11] Most interesting, however, is what both those planning to reenlist and to separate listed as the most influential reasons for their decisions. Of those who chose to reenlist, job security, medical benefits, retirement pay, and education and training opportunities were their primary influencers—albeit with a relatively increased influence of bonuses and special pays for those completing their first enlistments. For those Airmen who intended to separate, civilian job opportunities, pay and allowances, bonuses and special pays, promotion opportunities and the evaluation system contributed most heavily to their decisions (figs. 6 and 7).[12]

This information is extremely valuable. A Defense Manpower Data Center study was conducted between 2003 and 2005 on the stated intention of active duty enlisted members to reenlist or separate. It found that 95 percent of those who said they would reenlist at the beginning of the study did so at the end of the study period, while 23 percent of those who said they intended to separate did so.[13] Other studies in the private sector have similar findings. Specific comments from Airmen surveyed are illustrative of overall survey findings. Several Airmen stated that they were choosing to separate—regardless of pride and love of serving in the Air Force—because they felt that their skills were not being fully utilized. Also, they were aware they had the ability to earn more income for their families in the private sector. With bonuses and special pays listed as the third influencer for those choosing to separate, current SRB bonuses may not be enough to influence this group to reenlist. It is also interesting that many of those who say that they *will* reenlist included optimistic comments that they hope "someday" they may be able to apply the cyber skills they have attained in the service of the nation. This sense of lost utility in skills may be something worth monitoring. It may reflect a disconnect between Airmen's expectations and the reality of 1B4 mission contributions or the general effect from the sudden growth of the mission and career field that has yet to stabilize. If this trend continues, it may raise some caution to increasing accessions into the training pipeline until missions have stabilized and 1B4s are fully utilized for their mission.

AFSC 1B4X1 SEPARATION FACTORS BY TAFMS[a] GROUPS (AVERAGE RESPONSE SCORES)

[a]Total active federal military service

Separation Factors	First Enlistment N = 32	
	Percent Members Responding	Degree of Influence
Additional Duties	8	2.00
Base Housing	*	*
Base Services	*	*
Bonus or Special Pay	**41**	**2.38**
Childcare Needs	3	3.00
Civilian Job Opportunities	**66**	**2.52**
Enlisted Evaluation System	**34**	**2.00**
Equal Employment Opportunities	3	3.00
Esprit de Corps/Morale	25	2.25
Job Security	13	1.75
Leadership at Unit Level	28	2.56
Leadership of Immediate Supervisor	16	2.20
Location of Present Assignment	31	2.60
Medical or Dental Care for AD Member	6	3.00
Medical or Dental Care for Family Members	6	3.00
Military Lifestyle	22	2.71
Military Related Education and Training Opportunities	6	3.00
Number of PCS Moves	19	2.67
Number/Duration of TDYs or Deployments	6	2.50
Off-Duty Education and Training Opportunities	16	2.40
Pay and Allowances	**44**	**2.57**
Promotion Opportunities	**41**	**2.54**
Recognition of Efforts	16	2.20
Retirement Benefits	16	2.00
Senior Air Force Leadership	25	1.75
Spouses Career	*	*
Training/Experience of Unit Personnel	9	1.67
Unit Manning	9	1.67
Unit Readiness	9	2.00
Unit Resources	9	2.00
Work Schedule	16	1.60

* = No calculation available since factor was not selected
Note: Numeric values highlighted in blue indicate a top factor for that TAFMS group

Figure 6. 1B4X1 separation factors. (Data provided by CMSgt John Sanders, 1B4X CFM, SAF CIO A6/A6SF, 15 March 2015.)

COMPARISON OF AFSC 1B4X1 REENLISTMENT FACTORS BY TAFMS[a] GROUPS
(AVERAGE RESPONSE SCORES)

[a]Total active federal military service

Reenlistment Factors	First Enlistment N = 138		Second Enlistment N = 22	
	Percent Members Responding	Degree of Influence	Percent Members Responding	Degree of Influence
Additional Duties	6	1.75	5	1.00
Base Housing	3	1.50	5	2.00
Base Services	8	1.64	9	1.50
Bonus or Special Pay	30	2.48	23	1.80
Childcare Needs	3	2.25	5	3.00
Civilian Job Opportunities	24	2.27	36	2.00
Enlisted Evaluation System	5	1.86	9	2.00
Equal Employment Opportunities	*	*	*	*
Esprit de Corps/Morale	18	2.36	9	2.50
Job Security	48	2.53	41	2.33
Leadership at Unit Level	9	2.54	18	2.50
Leadership of Immediate Supervisor	9	2.54	18	2.25
Location of Present Assignment	12	2.31	14	2.33
Medical or Dental Care for AD Member	28	2.67	23	2.40
Medical or Dental Care for Family Members	33	2.70	36	2.75
Military Lifestyle	21	2.41	14	2.67
Military Related Education and Training Opportunities	22	2.48	14	1.67
Number of PCS Moves	4	2.33	5	2.00
Number/Duration of TDYs or Deployments	3	2.50	5	3.00
Off-Duty Education and Training Opportunities	30	2.52	27	2.17
Pay and Allowances	28	2.41	18	2.50
Promotion Opportunities	15	2.33	18	2.75
Recognition of Efforts	12	2.06	5	3.00
Retirement Benefits	53	2.74	50	2.64
Senior Air Force Leadership	5	2.14	5	3.00
Spouses Career	4	2.40	*	*
Training/Experience of Unit Personnel	20	2.44	14	2.67
Unit Manning	2	2.67	5	1.00
Unit Readiness	3	1.75	*	*
Unit Resources	4	2.60	5	1.00
Work Schedule	12	2.06	5	2.00

* = No calculation available since factor was not selected
Note: Numeric values highlighted in blue indicate a top factor for that TAFMS group
Note: Factors highlighted in yellow indicate that factor is a top factor across all three TAFMS groups

Figure 7. 1B4X1 reenlistment factors. (Data provided by CMSgt John Sanders, 1B4X CFM, SAF CIO A6/A6SF, 15 March 2015.)

Thus far we have discussed the evolution of the 1B4 career field to its present state as well as its future trajectory. Current retention trends do not appear to be meeting internal targets, but they are neither entirely out of step with the greater Air Force's retention trends nor indicative of great numbers of 1B4 Airmen preparing to jump ship in the near future. However, the rapid expansion

of this developing mission begs the Air Force to maintain as many cyber-capable Airmen as possible—particularly in light of the growing demand for cyber-skilled Airmen. We next look at specific options to reshape, grow, and retain a sustainable 1B4 cyber force for the future.

Notes

1. Healey, "Lost Cyber Heritage," 11–19.
2. Pawlyk, "Safest Job in the Air Force?"
3. CMSgt John Sanders (1B4X CFM, Secretary of the Air Force, Office of Information Dominance and Chief Information Officer [SAF/CIO] A6/A6SF), and MSgt Joseph Cochran, interviews by the author, Washington, DC, 11 and 15 March 2015.
4. Sanders, interview; and Rhonda Hutson (chief, cyber training, Air Force Space Command/A2/3/6), telephonic interview by the author, 16 March 2015.
5. "Interactive Demographic Analysis System (IDEAS)."
6. Hutson, interview.
7. Capt Christopher Price and 2d Lt Gregory Renner (Headquarters USAF/Deputy Chief of Staff, Personnel; Directorate of Force Management Policy; Force Management Division [HQ USAF/A1PF]), interviews by the author, Andrews AFB, MD, 16 March 2015.
8. Sanders, interview.
9. Informal author discussion with Air Force Fellows colleagues in the 14D cyber officer career field, January 2015. MSgt Joseph Cochran expressed the same sentiment in discussion with the author, March 2015.
10. Sanders, interview.
11. Data from occupational analysis survey initiated and administered by CMSgt John Sanders, fall 2013.
12. Sanders and Cochran, interviews.
13. Defense Manpower Data Center, "Retention Intention Study."

Chapter 3

Retention

As we grow the cyber workforce and gain experience from the lessons learned, non-traditional management approaches may be required for a portion of the cyber workforce, allowing the development and mastery of their tradecraft. The Department may require special considerations to ensure the Services have the ability to recruit, train, and retain top personnel.

—FY 15 National Defense Authorization Act

Congressional Concerns about Cyber Retention

As the DOD and the whole of the federal government have labored to increase the cyber workforce in recent years, Congress has been keeping a close eye on the department to ensure this growth continues in a sustainable fashion. This keen focus was expressed in the FY 15 National Defense Authorization Act (NDAA), which required the secretaries of the military departments to provide a report to "assess whether the cyber mission warrants new officer and enlisted specialty designators that are distinct from communications, signal, and intelligence specialties, and whether recruiting, retention, and assignment of service members with cyber skills requires bonuses or special pay and incentives."[1] The department's responding report, dated 31 January 2015, had an overall optimistic tone, indicating that all services but the Navy now had individual military specialties for enlisted cyber operators. The DOD also committed to continue monitoring retention needs at both the service and DOD levels, stating that it was currently monitoring and offering retention incentives as the services had requested and offering the option of additional incentives if identified by the services.[2] However, this congressionally directed report was not an initial motivator for the Defense Department to look at these issues since it had previously identified these priorities. The 2013 DOD *Cyberspace Workforce Strategy* outlined six broad strategic focus areas to guide the department in building a knowledgeable and skilled cyber workforce in a sustainable and adaptable manner. The fourth focus area established in this plan is to "retain qualified personnel" using the following four strategies:

1. Provide career progression and meaningful challenges;

2. Offer training opportunities tied to retention and commitments;
3. Retain qualified performers via compensation programs; and
4. Identify and retain cyberspace leaders.[3]

Although the DOD acknowledged that compensating cyber-skilled individuals at levels available in the private sector may not be possible, it suggested that it could potentially counter this disadvantage by leveraging unique work experiences and DOD missions to draw and retain talent in the pool. The strategy also recognized that success in retaining first-generation cyber talent would lend to the positive recruitment of future generations of cyber warriors.[4] Historically, the DOD has used special and incentive (S&I) pays as a means of inducing personnel to remain on active duty when retention is threatened in a specialty. Compensation strategies certainly will continue to play a large role in the department's retention strategies in the future, but other retention tools and strategies may also need to be considered for retaining the Air Force's 1B4s and must be looked at in greater depth. Recent studies related to retention behaviors have sought to identify the most influential factors in today's society that motivate workers to leave their jobs as well as those that best enhance employers' abilities to keep their workers. Many of these indicate that pay and compensation are a less effective part of the overall retention strategy than expected. Thus, other retention-focused conditions and initiatives must be included to affect retention favorably for the long haul.

Contemporary Civilian Labor Market Study Findings on Retention Best Practices

Given the expected cost in the private sector for each lost employee of anywhere between 50 and 200 percent of the employee's annual salary, there is little question why so much emphasis has been placed on what makes employees walk from their jobs and how best to keep them.[5] One focus of current studies is the "disengaged employee"—a category of employee that research has proven to be at most risk for retention. According to the Towers Watson's 2012 Global Workforce Study, disengaged employees may be recognized and defined as those who score low in three broad categories. The first category—traditional engagement—is the degree to which employees willingly and without coercion are committed to the organization's goals. The second—enablement—includes employee perceptions of the work environment's support of productivity. The third—energy—is the extent to which a work environment contributes to employee well-being. On the flip side, a very engaged

employee would rate high in all three categories. The study reveals that only about 35 percent of employees could be categorized as engaged, with about 26 percent classified as disengaged. Disengaged employees all scored low in the sustainable engagement elements. Consequently, they lack pride in their employer, do not believe in the company and its goals, feel underequipped to effectively perform their jobs, and are often unable to maintain their energy due to a work/life imbalance. Further, disengaged employees are more than twice as likely to leave their employer as compared to engaged employees.[6] A study by Valerie Ford, Susan Swayze, and Diane Burly on retention trends of information technology (IT) professionals found a strong link between worker exhaustion (defined as employees who felt overworked) and disengagement, which in turn was highly connected to negative retention decisions.[7] Employees in a 2012 World at Work study cited opportunities for better pay and promotion and the perception of inequitable pay compared to the compensation of peers (factors that would presumably lead to disengagement) as the top three reasons that would drive them to ultimately quit their jobs.[8] While these results might lead us to believe that pay is a top motivator in the retention decision for employees, a 2015 RAND study surveying the public sector's retention strategies specific to cybersecurity professionals found that high pay was generally not a practice used to retain employees. Rather, more common strategies to support employee retention involve offering competitive median salaries coupled with creating and maintaining a challenging work environment that generates strong bonds among the employee, the organization, and the mission.[9]

This observation is well backed by other studies. It has become clear that the cultural and relational aspects of a workplace have more to do with long-term employment than do pay or other tangible facets of the employee/employer relationship. Identified best practices in retaining personnel include continually engaging with employees to ensure that they feel connected to their jobs together with focusing on maintaining a high-quality work experience for employees in which their contributions are clearly valued by the organization. The *2012 Global Workforce Study* found that 88 percent of highly engaged employees perceived a strong link between their job contributions and the larger organization's mission accomplishment.[10] This finding is worth highlighting because the link between employee contributions and the larger organizational effort was a constant, common theme for successful retention among all of the studies reviewed.

As the 2015 RAND study notes, pay has less impact on retention of cyber professionals than one would expect, leading one to ask what in fact influences their retention. Petros Rigas's study on retention of IT professionals indicates

that raising salaries did little to decrease turnover. Rather, taking actions such as reducing perceptions of work/life imbalance, creating a work environment that fosters innovation, and implementing other measures to improve the work environment were more effective.[11] This is not to say that his study implies that pay and other forms of compensation don't matter. Job security and pay were often rated high not only as reasons for initial attraction to an employer but also as a critical element of retention. Based on his study of hundreds of individuals working in IT positions across many organizations, Rigas concludes that the best practical strategies for organizations to retain such employees may be to decrease bureaucracy and to increase support of employee development through a focus on business- and mission-related contributions.[12] Nevertheless, further corroborating the importance of competitive compensation as a baseline retention requirement, the 2012 World at Work survey indicates that employers rate compensation near the top of their most used and effective retention tools for employees who are key to organizations or possess critical skills.[13]

One can generalize from these studies that compensation alone is not sufficient incentive for retaining employees. As a baseline requirement, however, compensation must be perceived as fair and competitive as compared to other employment options. Moreover, other "softer" factors such as job satisfaction, perceived workload, and personal contributions to the organization/mission must also be in proper alignment and, collectively, tend to have an overall greater effect in supporting retention. This study's final retention strategy recommendations are informed by the review of this literature on retention influencers. Also informing this study's findings is the next area investigated—the DOD's more traditional means of pay and compensation to support retention in the armed forces.

Department of Defense Retention Tools and Practices: Special and Incentive Pays

The DOD has intensified the use of S&I pays since 9/11, offering over 60 varieties ranging from compensation for certain skills and assignments to retention-related pay. These incentives give the service branches greater flexibility to manage the force and improve manning (accessions and retention) and readiness in a targeted manner. Today, the department's annual budget for pay and compensation is $3.7 billion.[14] Granted, this pay category is only 2.6 percent of the overall compensation budget, but $3.7 billion is a considerable amount of money. This cost has led some people to question whether

these special pays and bonuses have had the intended effect in shaping the force, supporting retention, and, ultimately, bolstering readiness. We will take some time providing background on what recent studies have found regarding the effectiveness of these tools and others in supporting retention and force management and how these findings might be applied to support the growth and retention of 1B4s.

While the use of S&I pays has fallen under some level of criticism, a rough framework does exist as provided in the *Eleventh Quadrennial Review of Military Compensation* (*QRMC*). It guides defense policy makers on how to determine potential appropriate applications of these tools to support retention and force management. This framework of criteria ensures that special pays are targeted toward the identified problem and for justifiable reasons. To be eligible for S&I pays, targeted groups should meet all or some of the following conditions:

1. High potential for civilian pay as compared to regular military compensation (RMC).
2. High replacement/training cost of lost military member.
3. Accelerated internal growth in skills demand.
4. Hazardous working conditions.
5. Special skill or ability.
6. Special performance (extremely rare).[15]

Targeting incentives to those individuals who meet these criteria provides the most efficient means of delivering incentives and inducing retention behaviors rather than across-the-board pay increases. Ultimately, the ROI in these pays is measured by the ability to influence behavior and should be evaluated on a regular basis to ensure they are having the intended effect.

The 11th *QRMC* also established several "stylized facts" regarding known and accepted trends in retention that are commonly understood and should be accepted as baseline retention behavior knowledge. The first of these facts is that retention is always lowest at the end of the first-term of enlistment. Second, retention rates continue to rise following the first enlistment up to the 20-year retirement eligibility point. This rise is attributed to two primary reasons. First, those who make an early decision to stay until retirement increase overall retention. Second, the longer personnel stay in active service, the greater the likelihood they will stay until retirement. The final stylized fact regarding retention trends is that upon retirement eligibility at 20 years,

retention drops precipitously.[16] Another notable trend is that retention has been proven to be influenced by civilian unemployment, although not as starkly influenced as recruiting, which historically has shown that both recruiting and retention suffer as unemployment drops.[17] These facts provide meaningful parameters when analyzing retention issues and making policy decisions regarding potential S&I pays to influence retention. However, these known trends alone do not provide the level of scrutiny needed to determine the potency of applying specific S&I pays to support a retention strategy.

Models to Measure Retention and Special and Incentive Pay Effectiveness

Two models are generally used to study retention, including analysis of the effect of special pay on retention decision making. The first is the annualized cost of leaving (ACOL) model. It considers those making a reenlistment decision as rational beings who evaluate the financial benefits of both staying in the service or leaving over a dominant timeline (typically 20 years) and choosing the option offering the highest annualized payback. A member's view of or taste for military service is also factored in relative to tangible compensation options. The model has been revised to include options for inputting random "shocks"—good or bad—to measure effects on either high or low views/tastes toward continued military service that potentially influence members' decisions to reenlist. One trend supported by this analysis is that regardless of "bad shocks" (i.e., undesirable assignment, deployments, etc.), those with high tastes for service generally continue to remain in service longer than those with low tastes, even if those with low tastes for service experienced fewer of these negative shocks.[18]

The dynamic retention model (DRM) is also widely used to predict retention behavior. Although similar to the ACOL model, the DRM uses the concept of "multiple horizons," which acknowledges that individuals will make retention decisions at multiple points of time. It also places different weights/distributions based on an individual's taste for service and accounts for any future changes to pay as factors that affect retention. The DRM is more complicated and requires more computing power, but it has been used more in recent studies to determine the cost/benefits of using S&I pays in the armed forces. The model's dynamic qualities are regarded as a more accurate predictor of retention decision behaviors.[19] With the additional options for predicting complex outcomes, the DRM has been used extensively to model the effects of S&I pays to support retention and justify S&I pay policy decisions.

General Findings on the Efficiency of Special and Incentive Pays in Supporting Retention

A RAND study employing the DRM to measure the effectiveness of SRB multipliers to support reenlistment decisions during the height of the wars in Iraq and Afghanistan found that SRBs positively affected reenlistment for both first- and second-term Airmen. However, the study also revealed that bonus increases had no effect on the length of reenlistment periods, a fact that it attributed potentially to service enlistment policies that did not offer sufficient motivation/compensation to induce extended reenlistment. Also notable is that the SRB's average cost of $70,000 per additional year of enlistment for the Air Force was far and away the highest of all the services. This difference was attributed to a smaller overall effect of SRBs on reenlistment behavior in the Air Force compared to the other services and the shorter length of enlistments per taker. Nonetheless, this finding does reflect some measure of efficiency in offering a bonus. This cost should be weighed against the alternative of not offering a bonus and accepting higher attrition if the cost of replacement is lower than the bonus. The average cost per additional year of service is often increased as many Airmen who would have reenlisted absent a bonus must also be paid if the bonus is offered (a cost often referred to as economic rent). This increase elevates the overall cost—particularly if the bonus does not sufficiently motivate the targeted additional on-the-fence Airmen to reenlist. The ultimate finding of this study is that SRBs increase retention in the Air Force but only very slightly and are most effective for those completing their first enlistment. Further, they are costly and not always as efficient as the Air Force would like.[20]

Growth and establishment of the remotely piloted aircraft (RPA) enlisted sensor operator (SO) 1UX career field draw many close comparisons to the expanding cyber mission and the introduction of 1B4 as a distinct AFSC. The growth of the latter, however, was spurred more by the drastically increased combatant commander appetite for intelligence, surveillance, and reconnaissance during the height of the global war on terrorism rather than by the reactive need to increase cyber capabilities to meet emergent threats to the nation. In support of this growth in RPA operations and the associate need to increase the number of operators, in December 2010 the Office of the Under Secretary of Defense for Personnel and Readiness (OSD/P&R) extended authority to the Air Force to offer career enlisted incentive pay (CEVIP) to SO Airmen. Although CEVIP equates to flight pays normally given to enlisted flight crews, it is targeted pay offered only when Airmen are filling RPA flight crew duties.

Normal enlisted flight pay is generally paid to Airmen regardless of current duty assignment.

As a condition for extending this authority, OSD/P&R required the Air Force to report on the "effectiveness and efficiency" of this and other potential incentive pays. RAND conducted an econometric report using a DRM variant model accounting for civilian employment pay and opportunities and factoring in the extended time to gain initial mission qualification training and experience—ranging from 20.5 to 24.5 months for SO operators. This report suggests that enlisted Airmen retention behaviors are usually more sensitive to differences in pay opportunities in the civilian sector than are officer behaviors. Moreover, once civilian wage opportunities reach 130 percent of RMC—defined as the combination of basic pay, an average basic allowance for housing, allowance for subsistence, and other federal income tax advantages—meeting retention and manning targets would be difficult and nearly impossible at a 140 percent gap.[21] Another measure of comparison for the 1B4s is the biannual US Bureau of Labor Statistics (BLS) release of occupational wage statistics by state and local area. According to the May 2013 report, the US median wage was $88,600 for information security analysts, who most closely coincide with members of the 1B4 occupation skill set. However, adjusting for the local labor markets where approximately 80–85 percent of 1B4s are in the San Antonio, Texas, or Washington, DC, metro areas, the median incomes increase to $89,800 and $106,200, respectively. Today, an average technical sergeant in the Air Force (E-6) with 10 YOSs has an annual RMC of $64,763, which includes base pay, basic allowance for housing, and a subsistence allowance as well as a calculation for federal income tax advantage.[22] Thus, US median pay for civilians compared to that of Air Force service members in equivalent IT jobs and with the same levels of experience is at 136 percent; for San Antonio, 138 percent; and for DC, 173 percent. It is also worth noting that (at the time of this writing) these BLS tables are nearly two years old and will soon be updated; based on the labor market environment described in the first chapter, these figures will likely increase. Using the DRM to predict the effect of incentive pays, this study presumed a pay gap of 140 percent. With the insertion of substantial SRB payments in the fourth, eighth, and 12th YOSs (presuming a four-year term of enlistment), the cumulative retention curve increased for RPA SOs from 5 to 10 percent for each YOS. When the report measured the efficiency of these bonuses—taking into account training costs in relation to the average civilian wage differential—it noted that higher training costs reached a break-even point at lower civilian wage gaps and a quicker ROI for bonus dollars expended. On the flip side, lower replacement training costs required a higher civilian wage gap to break even and realize savings. Ultimately,

the study recommends continued incentive pay for SO personnel, which is likely driven by the high cost and long training pipeline requirements associated with replacing losses.[23] The study further suggests reevaluating the effectiveness of incentive pays in three to eight years. According to SMSgt Kimberly Scott, career field manager for SO, Headquarters USAF, no reviews are currently under way to measure CEVIP's effectiveness. She further anticipates that this incentive pay will continue for the foreseeable future.[24] The use of CEVIP as a means of closing pay gaps and incentivizing personnel to go into the career field may have been an appropriate leap given that many of the initial cadre of Airmen who entered the RPA SO career field were former enlisted aviators. Creating parity between this group of Airmen and personnel being trained as SOs without previous manned flight experience made sense at the time. At this juncture, it may be worth studying the need to continue this pay to determine if it is in fact providing any ROI in supporting retention. Also, with respect to application for 1B4 Airmen, this form of incentive pay—with its inflexible and unwieldy nature—may not be the best fit for supporting the growth and retention of cyber Airmen in the long run.

Supporting this appraisal, an exploration of incentive pays to support the growth and expansion of the RPA mission and RPA operators in the *Eleventh QRMC* suggests that using bonuses to increase retention was appropriate when rapid increases in requirements and high-cost or long training periods exist, even at the risk of inefficiency.[25] However, the *QRMC* proposes the use of flexible and adjustable bonuses such as SRBs over rigid career or skill pay bonus options because they are more easily adjusted to environmental conditions and retention behaviors. It further recommends that services take a "systematic approach" to analyzing the need for S&I pays when introducing new occupations with growing requirements and that they consider the following:

1. Conducting a thorough civilian labor market survey that includes civilian earnings potential.
2. Assessing whether S&I pay framework criteria are met by the new occupation as described earlier, such as increased requirements, long-term or high-cost training, dangerous work conditions, or needed skill acquisition.
3. Analyzing whether a cross-train bonus may be appropriate to motivate personnel to fill needed growth gaps.
4. Avoiding inflexible career or skills pays in the absence of similar portable civilian occupations and available recruiting or retention data.

5. Collecting trend data to monitor retention and evaluate the need for changes in retention tools and policy.[26]

Applying this systematic approach to what is currently known about cyber-skilled military personnel would lead one to believe that even though the use of S&I pays may certainly be appropriate, it would require additional and constant monitoring of retention trends to complete the justification.

A US Air Force Academy study aimed at predicting the SRB multiplier efficiency as well as retention rates for each AFSC used another variant of the DRM to provide the Air Force Force Management Division (AF/A1PF) with additional analytical rigor behind SRB multiplier policy decisions.[27] It targeted Airmen facing a retention decision within a fiscal year and considered the quantitative relationship between zip-code-level economic conditions (e.g., unemployment and inflation) and multiple AFSC-level demographics. The study found that, as a whole, an increase in the multiplier by one would increase retention by only 1 percent (estimated) overall across all zones. Also, for the most part, only Airmen in Zone A AFSCs who historically had not received bonuses or Airmen reaching their dates of separation showed any significant increase in retention with the use of the SRB. Further, the study detailed recommendations for maximizing the overall efficiency of the SRB program budget. These include (1) using the model's outputs to justify reducing SRB use for AFSCs with high forecasted retention costs, (2) fixing SRB multiplier levels more efficiently by targeting them at the level the model estimated would be needed to retain targets, and (3) reducing or eliminating SRB targets for AFSCs that the model predicted would meet targets absent the bonus. However, as a general statement, the study indicates that certain economic and other environmental factors leading to labor supply shortages could give cause for a more prolific targeted use of bonuses. It also mentions, though, that applying the above tactics was not usually as cost effective as desired and that their effects would need to be evaluated and adjusted annually.[28]

Each fiscal year since the completion of this study, AF/A1PF has collaborated with the study leads to use this model for outputs to help inform SRB multiplier decisions. Interestingly, the output using this model for FY 15 to predict retention and the ideal SRB multiplier for 1B4s suggests that an SRB not be offered to any zone to increase retention. Researchers believe that the model's output was based on the cost of inducing additional years of service versus replacing losses favoring the efficiency of taking additional losses over offering a bonus. Nevertheless, as noted earlier, SRBs are in fact being offered to 1B4s in FY 15, presumably due to the manning shortages magnified by the increasing authorization growth each FY and the current shortfall in meeting

retention goals. The risk of not offering an incentive may be too great, and the Air Force may be better off inducing the retention of as many 1B4 Airmen as possible, regardless of the efficiency costs.[29]

In light of the tendency noted earlier for 1B4 retention to drop precipitously at 20 YOSs, it may be in the Air Force's interest to look at options for increasing the number of senior enlisted personnel beyond retirement eligibility to retain a bench stock of experienced cyber operators to serve in critical positions and support the growth and maturation of the career field. John Warner indicates that critical skills retention bonuses (CSRB) have been used prolifically for special operations forces (SOF) retirement-eligible personnel to increase service beyond 20 YOSs, particularly during the height of the wars in Afghanistan and Iraq. In his report on the effectiveness of the CSRB on SOF retention, Warner notes that the CSRB options were very generous, which for Army SOF required a minimum two-year to a maximum six-year commitment—with bonuses increasing incrementally from $18,000 to $150,000. The DRM determined that the CSRB substantially increased retention for personnel with 19 to 24 YOSs from 17.3 to 37 percent, for an average service length of 4.5 years for takers. However, Warner points out that these additional years of service were extremely costly—driven mainly by the large incremental bonuses per year of service and coupled with the effect of economic rents as well as the additional retirement benefits incurred by additional YOSs.[30] While CSRBs proved to lengthen careers for retirement-eligible personnel, the success of this program should be weighed by the organization's value of retaining highly experienced personnel versus the cost of retaining them for longer periods.

Other less direct types of incentive pays, in the form of payments in kind, have also been recognized as an effective means of supporting retention of personnel within the DOD. A study using the DRM to predict the long-term retention effects of the Army's Graduate School for Service Program (GRADSO) predicts progressive retention benefits. Targeted to junior officers several years ago, GRADSO funds two years of graduate school for Army officers on active service, followed by a three-year ADSC upon completion of the program. In fact, this program has been so successful that the Army eventually capped participants at 300 yearly. Used to measure the program's effectiveness, the DRM predicted that program participants would have much longer careers and be more likely to reach retirement eligibility compared to other officers. In fact, the model projected that the year groups in the program may have increased retention beyond the Army's future requirements for the respective year groups, a possibility that bears watching in future years. Overall,

this study summarized that in-kind benefits tied with ADSCs are also effective options for retention and force management.[31]

Retention models and studies vary in their assessments of the effectiveness and efficiencies of S&I pays and other retention tools historically used in the DOD, but research cited in this study and the author's interactions with pay policy personnel in the Pentagon suggest that S&I pays will continue to play a role in supporting retention and shaping the force. The information in this chapter and the picture of the current environment for 1B4s prompt the next chapter's final analysis and recommendations to support 1B4 growth and retention.

Notes

1. S. Rep. 113-176, *National Defense Authorization Act*, "Cyber Career Field," 118.
2. Ibid., 1, 4.
3. DOD, *Cyberspace Workforce Strategy*, 6.
4. Ibid., 13–14.
5. Scott, McMullen, and Royal, *Retention of Key Talent*, 2.
6. Towers Watson, *2012 Global Workforce Study*, 2, 4–5, 9.
7. Ford, Swayze, and Burly, "Disengagement, Exhaustion and Turnover," 56–57.
8. Scott, McMullen, and Royal, *Retention of Key Talent*, 8.
9. Schmidt et al., *Cyber Practices*, 49–51.
10. Towers Watson, *2012 Global Workforce Study*, 13.
11. Rigas, "Model of Turnover Intention," 5.
12. Ibid.
13. Scott, McMullen, and Royal, *Retention of Key Talent*, 66.
14. Office of the Secretary of Defense (OSD)/Military Personnel Policy (MPP)/Compensation Branch, briefing slides.
15. Hogan et al., "Special and Incentive Pays," 108–9.
16. Ibid.
17. Ibid.
18. Ibid.
19. Wozny et al., *Selective Retention Bonus*, 1–18.
20. Asch et al., *Cash Incentives*, 101–3.
21. DOD, "Military Compensation."
22. Ibid.
23. Hardison, Mattock, and Lytell, *Remotely Piloted Aircraft*, 65.
24. Scott, telephonic interview by the author, 12 March 2015.
25. Office of the Under Secretary of Defense, *Eleventh Quadrennial Review*, 130–32.
26. Hogan et al., "Special and Incentive Pays," 131–32.
27. Wozny et al., *Selective Retention Bonus*, 1–18.
28. Ibid., 47–48.
29. Ibid.
30. Warner, "Effect of CSRB," 194–98.
31. Mattock et al., *Management of Officer Retention*, 31–36.

Chapter 4

Final Analysis and Recommendations

As adversaries exploit the Cyberspace domain for their military, economic, and political advantage, operations in cyberspace are evolving from an afterthought to a fundamental element for achieving all missions. The Department must similarly evolve the workforce to address the needs of the domain.

—Ashton Carter
Department of Defense Cyberspace Workforce Strategy

Review of Findings

As we begin the final analysis and provide final recommendations to enhance future 1B4 growth, retention, and overall health, let's first review the highlights of this study's findings:

1. Cybersecurity skilled personnel are in extremely high demand in the civilian labor market. The market has been in short supply for quite some time and is expected to remain so for at least the next 5–10 years. One study, however, is predicting that labor market demand and supply may reach equilibrium in fewer than 10 years.
2. Cyber Airmen, in particular 1B4s, have the skill sets needed in the labor market: their skills are extremely portable and in high demand.
3. The Air Force has experienced a tremendous requirements growth for 1B4s in recent years and expects the growth in authorizations for 1B4s to continue through FY 16, largely to support the Air Force contribution to cyber mission forces under the control of USCYBERCOM.
4. The 1B4 AFSC is currently manned at 46 percent of authorizations and is presently accessed only through cross-training, with the average minimum mission qualification training pipeline averaging 8–14 months per trainee depending on unit/mission assignment and other factors. Airmen incur a three-year ADSC upon attaining 3-level. Training throughput has been expanded and will need to continue to expand to meet bow wave requirements. Average cross-train YOSs for the current

group in the training pipeline are 6.8 (average rank of staff sergeant). As career field growth stabilizes and reaches sustainment, the Air Force wants to introduce new accessions into the career field.

5. Retention for 1B4s parallels that of the Air Force but falls short of prescribed career field retention goals that support career field growth. Although the field doesn't have a long history of trends to analyze, existing trends demonstrate that retention may be slipping. Retention decision impacts are greatest at 12–13 YOSs and at retirement eligibility with 20 YOSs.
6. Retention intentions as measured in the occupational analysis survey are not alarming but do indicate a certain expectation disconnect. Comments from 1B4s reflect a common view of not being used as they expected in the mission for which they were trained. Of those who chose to reenlist, job security, medical benefits, retirement pay, and education and training opportunities primarily affected their decisions to stay. Those completing their first enlistment were relatively more influenced by bonus and special pays. For those Airmen who responded with an intention to separate, civilian job opportunities, pay and allowances, bonus and special pays, promotion opportunities, and the evaluation system contributed most heavily in their decisions to leave. These findings regarding what 1B4s value most provide great insight into strategies for retention and growth in the field.
7. SRBs have increased for 1B4s in recent years but, on the surface, do not appear to be greatly influencing retention.
8. Rapid growth and unclear career paths / progression and developmental requirements for 1B4s are future challenges.
9. Contemporary civilian studies indicate that initiatives encouraging employees to remain highly engaged with the organization are a best practice in retaining personnel. Pay affects retention to a lesser degree from an employee perspective, but employers believe competitive pay is a critical tool in retaining personnel.
10. The use of S&I pays has been the DOD's primary tool to directly support force management, retention, and readiness. The effectiveness and efficiency in using such tools have been measured in various ways with mixed results. The overall sense is that while S&I pays do play a somewhat effective role in supporting force management at various points in the career life cycle, they are not always very efficient.

11. Flexible retention S&I pay tools that may be adjusted to environmental factors are preferred over career- or skill-related pays.
12. S&I pays should be considered to support the development of new occupations, particularly during rapid growth in requirements.
13. Other in-kind benefits with associated ADSCs offer an alternative to increasing retention / average career length as an alternative to S&I pays.

Final Analysis and Recommendations

This study's recommendations are intended to provide insights into how to support the 1B4 career field as it transitions from rapid growth to stability and, ultimately, sustainment. This new career field has many challenges ahead since it must increase manning in the short term but at the same time look to future sustainability. At present, 1B4s appear to be on the right path; over an extended period of time, they will be able to fulfill manning requirements through the career life cycle to meet sustainability. The recommendations are intended to influence reshaping the sustainment line for 1B4s toward a traditional sustainment curve to support the long-term growth and sustainability of the career field. They are also intended to support retention and to fill manning gaps below the sustainment line as the line is being reshaped. These goals require influencing the curve along the entire length of the sustainment line, specifically targeting enhancements from accessions, to midcareer / Zone B retention, and through retirement eligibility and beyond. The summary findings noted above help inform these recommendations.

First, the Air Force should adjust accessions and ADSC policy for 1B4s. An incremental move toward a hybrid accessions model, similar to the paralegal career field (5J0X1), requires a minimum six-year ADSC upon attainment of 3-level training. In the short term, cross-training personnel will still be necessary to meet growing requirements. However, incrementally introducing new accessions while simultaneously tightening the parameters for cross-training into 1B4 would create opportunities for longer careers and build a more sustainable stand-alone career field that supports developing more experienced cyber experts. One recommendation is to infuse new accessions slowly, increasing 10 percent of total accession requirements per year until reaching a total of 50 percent of annual accession requirements. Further recommended is reducing the YOS cap for cross-trainees by two YOSs each year starting in FY 16 through FY 19 until the maximum YOSs for cross-training are set at six. Also, the career field should investigate directing the majority of the cross-training pipeline from cyber support AFSCs in the 3D0 series. Doing so creates a natural minor-league pathway of sorts for those young accessions

who may show a proclivity for cyber operations but may need more time to mature as Airmen. Implementing these recommendations would reshape the sustainment curve of the career field to a more traditional and sustainable shape that depends less on cross-trained noncommissioned officers (NCO), as demonstrated in the 5J0X1 CFH chart (fig. 8).

Second, the Air Force should maintain an SRB multiplier at current levels for 1B4s but work with RAND personnel or other analysts to run DRMs specific to 1B4s, taking into account current and forecasted civilian labor market indicators and realistic pay gaps. Although studies have shown that SRBs may not be efficient and economic rent may be high, the fallout risk of reducing or eliminating SRBs for 1B4s is too great considering the voracious civil labor market climate and the concurrent requirement for the Air Force to grow the career field. At the same time, however, the study recommends that the Air Force not pursue any further special duty pays or other career- or skills-linked special pays at present because once such pays are introduced, they are difficult to reduce or eliminate. Rather, the Air Force should concentrate the current SRB S&I pays on early and midcareer personnel for whom SRBs offer greater flexibility to adjust to environmental factors and support retention. Finally, to facilitate growth and retention at the top/left of the sustainment line, offering sufficient bonuses to Zone A new accessions and cross-trainees when they attain their 3-level would support needed cross-flow personnel and longer ADSC commitment requirements upon initial training completion (six years). Offering higher-level bonuses to Zone B reenlistments would also support this goal although it has been noted that Zone B reenlistments are generally not as greatly influenced by SRBs. This investment in Zone B may have a higher economic rent cost but could be a worthwhile long-term investment.

Third, to keep its most experienced and skilled Airmen, the Air Force should also consider introducing CSRBs for those reaching retirement eligibility in the near term. CSRBs should be given only at moderate levels, and the number of bonuses should be capped to better manage the force and encourage some level of competitiveness for additional years of service. At present the group most affected with decreased retention is Airmen reaching retirement eligibility—the vast majority of personnel who reach 20 YOSs exit the service. Although promotion opportunity has increased in recent years, few 9-level positions are available for 1B4s. Many 7-levels who reach retirement eligibility and have little hope for promotion tend to retire immediately since they have no incentive to stay in the service. Extending the bench of cyber experts with deep experience in their tradecraft will be important for the career field as it attempts to stabilize. Prior to implementing this measure, additional analysis must be completed to determine the number of personnel desired to extend beyond 20 YOSs and establish the right cap level and incremental bonuses for each YOS.

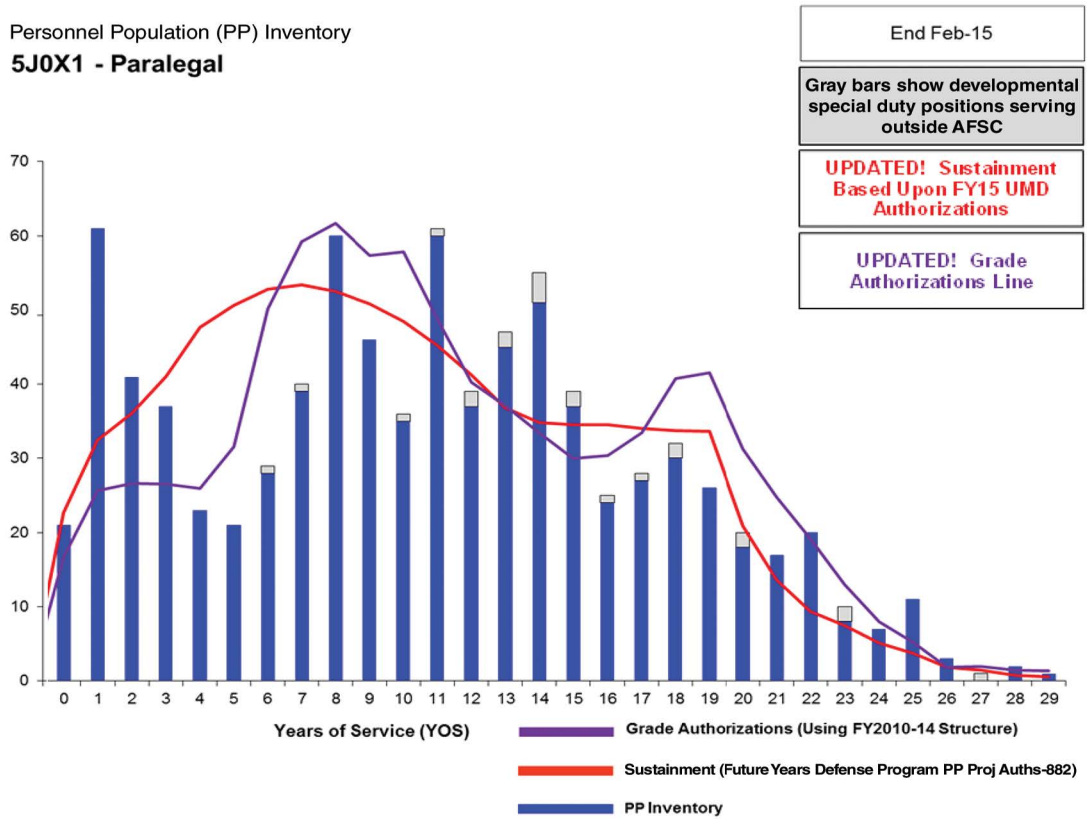


Figure 8. Paralegal career field (5J0X1) sustainment as of February 2015. (Provided by Headquarters USAF/Deputy Chief of Staff, Personnel; Directorate of Force Management Policy; Force Management Division [HQ USAF/A1PF].)

Third, to keep its most experienced and skilled Airmen, the Air Force should also consider introducing CSRBs for those reaching retirement eligibility in the near term. CSRBs should be given only at moderate levels, and the number of bonuses should be capped to better manage the force and encourage some level of competitiveness for additional years of service. At present the group most affected with decreased retention is Airmen reaching retirement eligibility—the vast majority of personnel who reach 20 YOSs exit the service. Although promotion opportunity has increased in recent years, few 9-level positions are available for 1B4s. Many 7-levels who reach retirement eligibility and have little hope for promotion tend to retire immediately since they have no incentive to stay in the service. Extending the bench of cyber experts with deep experience in their tradecraft will be important for the career field as it attempts to stabilize. Prior to implementing this measure, additional analysis must be completed to determine the number of personnel desired to extend beyond 20 YOSs and establish the right cap level and incremental bonuses for each YOS.

As the research cited in this study suggests, S&I pays alone often are not an efficient means of influencing retention, particularly when a career field is in a state of growth. A more diverse retention portfolio is necessary, including civilian education and development opportunities linked to associated ADSCs. Primarily targeting Zone B Airmen who often are the least influenced by S&I pays may increase overall retention efficiency and outcomes. Currently, 1B4s have only limited development options. One is to apply for the Computer Network Operations Development Program (CNODP), a three-year NSA internship that incurs a three-year ADSC upon completion, or to obtain an AFIT cybersecurity degree. A second option is a two-year graduate-level degree program, which would require a similar ADSC. Recently, however, only one or two slots per year have been open for each of these opportunities: 1B4s as well as other AFSCs are eligible to apply. Moreover, low manning has led to some difficulty in releasing personnel to these programs. SRBs may have limited effect in supporting retention of Zone B personnel. A more effective tool may be to expand education and development opportunities exclusive to cybersecurity (1B4s), with a minimum two-to-one-ratio follow-on ADSC tied to such programs. This study recommends that these educational programs follow along the lines of the Air Force Institute of Technology (AFIT) civilian institute construct in which AFIT partners with reputable public and private universities with strong cyber programs, including the 12 NSA-certified universities offering cyber surety degrees. These programs should also include partnerships with industry, similar to the officer-education-with-industry programs. Companies such as Google, Oracle, and J. P. Morgan—and others on the leading edge of cybersecurity in the private sector—would be good

partners for developing Airmen. Partnering with these companies could possibly involve an exchange program in which private-sector cybersecurity employees work temporarily within the Air Force / DOD. The objective would be to expand these programs to as many cyber Airmen as are willing; they must have promotion potential and be able to break away and attend these education/developmental programs. The ROI for such programs would go well beyond increasing retention by enhancing the competency and expertise of the cyber force.

This study recommends that the Air Force continue to conduct the occupational analysis survey biannually and to collect retention intention information from the field as a means of providing decision makers and career field managers with actionable information. As the service's cyber mission force continues to expand, it will be critical for the 1B4 CFM to maintain situational awareness not only of how 1B4s are being used but also of their intentions and motivations regarding staying in or leaving the Air Force. Since cyber operations are a new and evolving capability, adjustments will inevitably be made to how 1B4s conduct and contribute to the mission. Such changes will affect their career paths and future development requirements. Also, monitoring retention trends in this survey will prove useful; a recent study has shown a strong link between turnover and respondents' stated intentions to stay, as measured by a survey.[1] Thus, this data should provide a good prediction of future retention behavior to inform special pay and incentive policy and to make other policy adjustments to support retention as needed.

Also, linked to the above recommendation, establishing a 1B4 NCO advisory council would provide for a two-way flow of information from the field to CFMs and other decision makers. Doing so would increase awareness of the internal and external environment. This advisory council should be guided by a charter document establishing council leadership positions and regional- or unit-level representative positions. It should meet at a minimum on a quarterly basis (virtual, if required), with a clear and directive focus on developing a commonly understood career path/progression as the career field moves from growth/expansion to stability and sustainment.

Further, the council should focus on building and supporting Air Force cyber culture and traditions. Introduction of the cyber operator badge is an example of a visible cultural symbol for cyber operators, but this effort was somewhat tarnished when the initial guidance for awarding the badge permitted personnel with any AFSC to wear it, regardless of assignment/duty, as long as they were able to complete a computer-based online course available to anyone. This oversight caused frustration within the 1B4 community since many viewed this practice as "cheapening" their contributions, and it was broadly commented on in the occupational analysis survey. Although a new

badge-wear policy will rectify the situation in the coming years, the damage has to a certain degree been done. The advisory body's focus on building culture within the cyber forces and elevating oversights that degrade culture, such as the badge policy, would do much to support indoctrinating Airmen into and engaging them with the Air Force cyber forces.

Finally, this study recommends that career field leaders continue to collect as much information as possible on retention trends. Because the 1B4 career field is still in its infancy, there is a distinct lack of historical data trends to compare and contrast to current retention trends. Therefore, expanding data collection to include qualitative information—such as exit interviews of separating and retiring personnel in an effort learn more about 1B4 concerns and behavioral trends—will be critical to understanding and interpreting data lacking in historical context. Information could be quickly collected in real time with commercially available Web tools available at sites such as tinypulse.com. These tools would allow gauging organizational morale and culture and thus provide data that could be used to infer retention trends, enabling career field leadership to institute proactive measures rather than reactive/crisis management.

The preceding recommendations offer several options to positively influence 1B4 growth and retention given current authorities and previously used and practiced personnel policies, but they may still fall short of what is needed to build the Air Force's and the nation's cyber mission forces. The criticality of supporting the DOD's cyber workforce enterprise growth without any encumbrance was clearly a prime motivating factor behind the Force of the Future initiative that Secretary of Defense Ash Carter kicked off in late March 2015, just five weeks into his tenure. During a two-day domestic speaking tour in Pennsylvania and New York, he expressed his concern over the DOD's ability to field needed personnel with the skills demanded by the evolving nature of warfare. Secretary Carter stated, "But uppermost in my mind is ensuring that we have in generations to come what today gives us the finest force the world has ever known. And that's not our technology—that comes second. It's our people."[2] His speeches often use examples of the department's constrained ability to attract, recruit, grow, and retain cyber-minded professionals, whether they wear uniforms or serve as DOD civilians.

In my final few months as an Air Force fellow assigned to OSD P&R, I became heavily involved in the initial rollout effort for Force of the Future and was fortunate enough to hear the intentions of this initiative directly from senior defense policy makers. Secretary Carter's clearly stated objective for the Force of the Future initiative is to identify the adjustments necessary to current personnel practices, policies, or statutes to guarantee that the United

States can field the world's best military force consisting of the best possible human capital. He believes that we must act today with the intention of removing those institutional barriers that detract from this effort.

Secretary Carter charged his newly appointed acting undersecretary of defense for personnel and readiness, former congressman Brad Carson, to scrutinize current personnel policies governing all points of the Total Force military career life cycle for both officer and enlisted personnel. The areas included recruiting and accessions, career progression, performance evaluation, and retention—specifically, the department's ability to support the growth and retention of critical technical skill requirements such as cyber to assure that future policies fully enhance the desired attributes of tomorrow's force. The timeline to deliver findings and recommendations to Secretary Carter by the fall of 2015 reflects his awareness of the urgency of such reforms to bolster cyber mission force growth and sustainability and of the need for bold action using pioneering personnel policies. Any new authorities or policies recommended under Force of the Future may completely change the game, offering fresh and untested personnel management capabilities that must be reviewed and attempted as additive or enhancing to the previous recommendations to increase the Air Force's capacity in growing enlisted cyber personnel.

The high-profile nature of the Force of the Future initiative also demonstrates the zero-sum-game scenario of cyber warfare and the criticality of building adequate cyber forces to provide the necessary advantage. The secretary recognizes the potential inadequacies of the department to compete for cyber talent and understands that failure to take action could lead to disastrous consequences for our nation. Given that failure in cyberspace is not an option, the Air Force must follow the secretary's lead. It must take bold action to use all reasonable means currently available to support 1B4 sustainability as outlined above while simultaneously harnessing the vision for enhanced personnel mechanisms and policies to reinforce future cyber forces.

Notes

1. Bothma and Roodt, "Turnover Retention Scale," 12.
2. Pellerin, "'Force of the Future.'"

Abbreviations

ACOL	annualized cost of leaving
ADSC	active duty service commitment
AF/A1P	Air Force Directorate of Force Management Policy
AF/A1PF	Air Force Force Management Division
AFIT	Air Force Institute of Technology
AFSC	Air Force specialty code
ASVAB	Armed Services Vocational Aptitude Battery
BLS	Bureau of Labor Statistics
CCR	cumulative continuation rate
CEVIP	career enlisted incentive pay
CFH	career field health
CFM	career field manager
CNODP	Computer Network Operations Development Program
CSIS	Center for Strategic and International Studies
CSRB	critical skills retention bonus
DOD	Department of Defense
DRM	dynamic retention model
FY	fiscal year
GDP	gross domestic product
GRADSO	Graduate School for Service Program
IQT	initial qualification training
IST	initial skills training
IT	information technology
NCO	noncommissioned officer
NDAA	National Defense Authorization Act
NSA	National Security Agency
OSD	Office of the Secretary of Defense
OSD/P&R	Office of the Under Secretary of Defense for Personnel and Readiness
QRMC	*Quadrennial Review of Military Compensation*

RMC	regular military compensation
ROI	return on investment
RPA	remotely piloted aircraft
S&I	special and incentive
SO	sensor operator
SOF	special operations forces
SRB	selective reenlistment bonus
TIS	time in service
UMD	unit manning document
USCYBERCOM	United States Cyber Command
YOS	year of service

Bibliography

Asch, Beth J., Paul Heaton, James Hosek, Francisco Martorell, Curtis Simon, and John T. Warner. *Cash Incentives and Military Enlistment, Attrition, and Reenlistment*. Santa Monica, CA: RAND Corporation, 2010.

Bothma, Chris F. C., and Gert Roodt. "The Validation of the Turnover Retention Scale." *Journal of Human Resource Managemen*t 11, no. 1 (2013): 1–12.

Bureau of Labor Statistics. "Fastest Growing Occupations." *Occupation Outlook Handbook*, 17 December 2015. http://www.bls.gov/ooh/fastest-growing.htms.

Cartwright, Gen James E. (panelist). Interview by moderator Bob Schieffer. Center for Strategic and International Studies-Schieffer Series Dialogues. "Securing Cyberspace in the 21st Century." Video, 00:53:10, 6 December 2011. http://csis.org/event/schieffer-series-who-commands-commons-securing-cyberspace-21st-century.

Center for Strategic and International Studies (CSIS) and McAfee. *Net Losses: Estimating the Global Cost of Cybercrime; Economic Impact of Cybercrime II*. Santa Clara, CA: Intel Security, June 2014.

Chen, Thomas M. *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*. Letort Papers. Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2013.

CISCO Systems. *Annual Report 2014*. Pursuant to sec. 13 or 15(d) of the Securities Exchange Act of 1934 for the fiscal year ended July 26, 2014. San Jose, CA: CISCO, 2014. http://www.cisco.com/web/about/ac49/ac20/ac19/ar2014/2014-cisco-annual-report.pdf.

Defense Manpower Data Center, Survey Technology Branch. "Analysis and Modeling Retention Intention Study." Briefing slides. Washington, DC: Department of Defense (DOD), 2007.

Department of Defense. *Department of Defense Cyberspace Workforce Strategy*. Washington, DC: DOD, 4 December 2013.

———. "Military Compensation: Regular Military Compensation (RMC) Calculator." Accessed 12 March 2015. http://militarypay.defense.gov/Calculators/RMCCalculator.aspx.

Evans, Karen, and Franklin Reeder. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. Report of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. Washington, DC: CSIS, November 2010.

Ford, Valerie, Susan Swayze, and Diane Burly. "An Exploratory Investigation of the Relationship between Disengagement, Exhaustion and Turnover Intention among IT Professionals Employed at a University." *Information Resources Management Journal* 26, no. 3 (2013): 55–68.

Fung, Brian. "You Call This an Army? The Terrifying Shortage of U.S. Cyberwarriors." *National Journal*, 25 February 2013. http://www.nextgov.com/cybersecurity/2013/02/you-call-army-terrifying-shortage-us-cyber warriors/61487/.

Hardison, Chaitra, Michael Mattock, and Maria Lytell. *Incentive Pay for Remotely Piloted Aircraft Career Fields*. RAND Project Air Force. Santa Monica, CA: RAND Corporation, 2012.

Healey, Jason. "Claiming the Lost Cyber Heritage." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012):11–19.

Hogan, Paul, Kim Darling, Patrick Mackin, Joseph Mundy, Meredith Swartz, and John Warner. "Analysis of Staffing and Special and Incentive Pays in Selected Communities." Chap. 4 in Office of the Under Secretary of Defense, *Eleventh Quadrennial Review of Military Compensation*.

Interactive Demographic Analysis System (IDEAS). Accessed 12 March 2015. https://w11.afpc.randolph.af.mil/RAW/asp/SecBroker/Drivers/Sec_Broker Transfer.aspx?_program=IDEAS%2ESec%5FIDEAS%5FDefault%2Esas&_service=prod2pool3%5Fsec&_debug=0&default_service=prod2pool3%5Fsec&SessionTransferId=28444FE8C717411CBFC6A27D333D73FCCA7IAXN1M.

Kay, David J., Terry Pudas, and Brett Young. "Preparing the Pipeline: The U.S. Cyber Workforce of the Future." *Defense Horizons* 72 (August 2012): 72–88.

Korn, Melissa. "Number of College Students Pursuing Science, Engineering Stagnates: National Push to Increase Workers' Skills Has Little Effect." *Wall Street Journal Online*, 27 January 2015.

Leonard, Bill. "Cybersecurity Professionals in Demand." *Society for Human Resource Management*, 22 June 2014. http://www.shrm.org/hrdisciplines/technology/articles/pages/cybersecurity-professionals-in-demand.aspx#sthash.jmjcMTpX.dpuf.

Libicki, Martin, David Senty, and Julia Pollak. *H4CKER5 WANTED: An Examination of the Cybersecurity Labor Market*. Santa Monica, CA: RAND Corporation, 2014.

Martinez, Luis. "Intel Heads Now Fear Cyber Attack More Than Terror." *ABC News*, 13 March 2013.

Mattock, Michael, Beth Asch, James Hosek, and Christopher Whaley. *Toward Improved Management of Officer Retention: A New Capability for Assessing Policy Options*. Santa Monica, CA: RAND Corporation, 2014.

Mickelberg, Kevin, Neal Pollard, and Laurie Schive. *US Cybercrime: Rising Risks, Reduced Readiness; Key Findings from the 2014 US State of Cybercrime Survey*. Industry Report. London: PricewaterhouseCoopers LLP, June 2014.

Office of the Secretary of Defense (OSD) / Military Personnel Policy (MPP) / Compensation Branch. Briefing slides. Provided to the author 15 March 2015.

Office of the Under Secretary of Defense. *Report of the Eleventh Quadrennial Review of Military Compensation: Supporting Research Papers*. Washington, DC: Office of the Under Secretary of Defense (Personnel and Readiness), 2012.

Pawlyk, Oriana. "Cyber: The Safest Job in the Air Force?" *Air Force Times*, 20 Feburary 2014. http://www.militarytimes.com/story/military/archives/2014/02/20/cyber-the-safest-job-in-the-air-force-/78543786/.

Pellerin, Cheryl. "Carter Details 'Force of the Future' at Syracuse University." *DOD News*. Defense Media Activity, 31 March 2015. http://www.defense.gov/News-Article-View/Article/604390/carter-details-force-of-the-future-at-syracuse-university.

Ponemon Institute LLC. *2014 Global Report on the Cost of Cyber Crime*: *Benchmark Study of Global Comp*anies. Sponsored by HP Enterprise Security. Traverse City, MI: Ponemon Institute LLC, October 2014.

Rigas, Petros Pavlos. "A Model of Turnover Intention among Technically-Oriented Information Systems Professionals." *Information Resources Management Journal* 22, no. 1 (2009):1–23.

Schmidt, Lara, Caolionn O'Connell, Hirokazu Miyake, Akhil R. Shah, Joshua Baron, Geof Nieboer, and Rose Jourdan et al. *Cyber Practices: What Can the USAF Learn from the Private Sector?* Santa Monica, CA: RAND Corporation, 2015.

Scott, Dow, Tom McMullen, and Mark Royal. *Retention of Key Talent and the Role of Rewards*. Scottsdale, AZ: World at Work, 2012.

"Significant Cyber Incidents since 2006." Center for Strategic and International Studies, 11 December 2015. https://web.archive.org/web/20160113213223/http://csis.org/files/publication/151211_Significant_Cyber_Events_List.pdf.

Spidalieri, Francesca, and Sean Kern. *Professionalizing Cybersecurity: A Path to Universal Standards and Status*. Newport, RI: Pell Center for International Relations and Public Policy, Salve Regina University, August 2014.

S. Rep. 113-176. Carl Levin National Defense Authorizaton Act for Fiscal Year 2015: Report to Accompany S. Rep. 2410. "Title V, Military Personnel Policy, Items of Special Interest, Cyber Career Field," 118. 113 Cong., 2d sess. Washington, DC: US Government Publishing Office, 2015.

Summers, DJ. "For Uncle Sam, Trouble Raising a Cyber Army." *Fortune*, 3 October 2014. http://fortune.com/2014/10/03/government-cyber-security-shortage/.

Towers Watson. *2012 Global Workforce Study: Engagement at Risk; Driving Performance in a Volatile Global Environment*. New York: Towers Watson, July 2012.

Warner, John T. "The Effect of the Civilian Economy on Recruiting and Retention." Chap. 2 in Office of the Under Secretary of Defense, *Report of the Eleventh Quadrennial Review of Military Compensation*.

———. "Evaluation of the Effect of CSRB Offered to Retirement- Eligible Special Forces Personnel." Chap. 5 in Office of the Under Secretary of Defense, *Report of the Eleventh Quadrennial Review of Military Compensation*.

White House. "The Comprehensive National Cybersecurity Initative," March 2010. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

Wozny, Nathan, Lt Col Justin Joffrion, Capt Nick Mastronardi, and Katherine Silz-Carson. *Impact of the Air Force Selective Retention Bonus Program on Retention*. Collaborative Report between HQ USAF and the United States Air Force Academy, 2013.

Yannakogeorgos, Panayotis. "Outbrief on AFRI [Air Force Research Institute] CSAF [chief of staff of the Air Force] Directed Study on Cyber Workforce Development." PowerPoint presentation. AFRI, Maxwell AFB, AL, 9 September 2014.

AFRI AU PRESS
AIR FORCE RESEARCH INSTITUTE
http://aupress.au.af.mil

ISBN 978-1-58566-264-7
ISSN 2329-5821