NIST Special Publication 1500-16

Improving Veteran Transitions to Civilian Cybersecurity Roles:

Workshop Report

Marian Merritt

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-16

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1500-16

Improving Veteran Transitions to Civilian Cybersecurity Roles:

Workshop Report

Marian Merritt
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-16

August 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Special Publication 1500-16
Natl. Inst. Stand. Technol. Spec. Publ. 1500-16, 25 pages (August 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-16

Abstract

The shortage of cybersecurity professionals is a significant risk to The United States of America's overall national security and economic prosperity. The U.S. branches of the military provide training and education in cybersecurity, and some transitioning military are well versed in risk management and may possess highly sought-after security clearances obtained while in the service. These trained, experienced, and often, able-to-be-cleared individuals should be viewed as highly desirable members of the civilian cybersecurity workforce. Yet, for some transitioning military it is challenging to determine how to translate military experience to civilian cybersecurity work roles and to find employers who have jobs that leverage their military experience.

A workshop was held on March 21, 2017, attended by a small group of interested participants from the federal government, non-profit organizations, academia, and industry, as well as several members of the military, to share information and ideas about how the environment might be improved before, during, and after transition programs.

Recommendations from the workshop discussion included concrete suggestions both for the military and for the private sector to do more to streamline a warfighter's experience from before entering the service all the way through to transitioning to a new civilian cybersecurity career.

Key words

career; civilian; cybersecurity; defense; military; training; transition; veteran; workforce.

National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology, is part of the U.S. Department of Commerce and is a partnership between government, academia and the private sector focused on cybersecurity education, training and workforce development. The three strategic goals of NICE are:

1. To accelerate learning and skills development
2. Nurture a diverse learning community
3. Guide career development and workforce planning

It is critical to address the cybersecurity workforce shortage and identify strategies to both speed the rate at which someone could qualify to enter the cybersecurity profession and encourage more diverse individuals to enter the field.

Executive Summary

The critical workforce shortage of cybersecurity professionals is a significant risk to the United States of America's overall national security and economic security. An estimated 4 million global cybersecurity jobs [1] are unfilled. Domestically, the estimate is closer to 508 000 open positions [2]. The shortage of talent is so large that (as estimated for the State of California) even if every student in a cybersecurity education or training program entered the field each year, there still would be a gap [3]. And the industry suffers low participation levels for women [4] and minorities [5]. Therefore, it's critical that every talent pipeline be considered for possible mechanisms that will encourage more people to pursue a career in cybersecurity.

Transitioning veterans may possess cybersecurity-related technical skills and experience, embody a commitment to the mission of protecting the Nation, and represent a relatively diverse population. As was stated in the co-authored Department of Homeland Security and Department of Commerce response to Presidential Executive Order 13800 on Strengthening the Cybersecurity of the Federal Networks and Critical Infrastructure, "*Veterans represent an available and underutilized workforce supply*" [6]. Veteran-hiring initiatives exist, both in and outside of industry, yet many of these programs are not discovered until too late by transitioning military.

Many veteran-hiring programs are local, underfunded, or limited in scale. Veterans may not find information about these programs, may not see how their military experience translates to job-readiness in the private sector, or may need assistance in gaining certifications necessary to qualify for some private-sector cybersecurity roles. A 2015 survey revealed that 40 % of veterans found their employment transition especially difficult [7]. An opportunity exists to build on existing programs, identify what is missing or ripe for improvement, and increase the speed to move our transitioned warriors to full employment in a rewarding cybersecurity career.

The NICE Veterans Workshop

On March 21, 2017, the National Initiative for Cybersecurity Education (NICE) convened a workshop in Rockville, MD with approximately 40 representatives of federal and state government, branches of the military, academia, industry, and workforce development organizations to explore issues, discuss initiatives, and better understand the challenges that keep veterans from transitioning to cybersecurity careers. This publication documents the findings of the participants from open discussion and guided-breakout sessions. Participants provided recommendations on how to increase visibility to cybersecurity as a potential career path for members of the military and their families and those in the transition programs. Workshop participants also described opportunities for those in the academic, government, and industry sectors to contribute to this effort.

Table of Contents

1. Findings of the Veterans Workshop

1.1. Background

The critical workforce shortage of cybersecurity professionals is a significant risk to the United States of America's overall national and economic security. An estimated 4 million global cybersecurity jobs [1] are unfilled. Domestically, the estimate is closer to 508 000 open positions [2]. The shortage of talent is so large that (as estimated for the State of California) even if every student in a cybersecurity education or training program entered the field each year, there still would be a gap [3]. And the industry suffers low participation levels for women [4] and minorities [5]. Therefore, it's critical that every talent pipeline be considered for possible mechanisms that will encourage more people to pursue a career in cybersecurity.

The NICE Veterans Workshop

On March 21, 2017, the National Initiative for Cybersecurity Education (NICE) convened a workshop in Rockville, MD with approximately 40 representatives of federal and state government, branches of the military, academia, industry, and workforce development organizations to explore issues, discuss initiatives, and better understand the challenges that keep veterans from transitioning to cybersecurity careers. The meeting included contributions of personal experiences of the participants, open discussion and guided-breakout sessions. Participants provided recommendations on how to increase visibility to cybersecurity as a potential career path for members of the military and their families and those in the transition programs. Workshop participants also described opportunities for those in the academic, government, and industry sectors to contribute to this effort.

Workshop participants agreed that cybersecurity is not well known or understood as a career field where military experience can qualify someone for future civilian career opportunities. More effort is needed to introduce military (and for the future, civilian) cybersecurity careers early in the military career or before military service. As the service member proceeds through their military career and transitions to the civilian workforce, they should be shown how their skills and education map to readily recognized standards for Tasks and Knowledge, Skills and Abilities (KSAs) [8] from the NICE Cybersecurity Workforce Framework (NICE Framework). Transitioning service members would benefit from well-informed coaching and guidance to help them: identify work roles; seek industry-recognized cybersecurity certifications; enroll in higher-education degree or certificate programs, finance their training and education, and receive benefits, scholarships and stipends.

1.2. Building Awareness of Cybersecurity as a Career

Awareness-building efforts can begin with programs and outreach targeted to the high school recruitment target population and to those just starting in the military. Outreach to young people (K-12) can feature cybersecurity as the sort of attractive and meaningful work done while in the military that directly translates to strong civilian careers with excellent earning potential. The military might add trained recruitment specialists or career counselors who

could address general cybersecurity awareness and mentions of military roles that include cybersecurity elements.

While in the military one can receive cybersecurity education, develop skills, and even receive funding to earn industry-recognized cybersecurity certifications. Military spouses and dependents should also learn about cybersecurity careers, especially when programs offering free or low-cost courses or online learning are available to them. Workshop participants discussed with enthusiasm the idea of featuring cybersecurity topics in on-base marketing channels (including posters, radio, and television spots on base channels such as Armed Forces Radio and Television programming). Participants suggested that materials and programs should feature success stories so that even those in technical, non-cybersecurity fields might be inspired to consider more options after they transition. However, it was made clear that programs should not contravene the military option of continuing in the service but be complimentary; showcasing multiple options for the service member, whether they remain in service or transition to civilian life.

1.3. Benefit of Veteran Employees

Veterans, when considered as an employee group, offer demographic and personality characteristics that are highly desirable in the cybersecurity workforce. For example, workshop participants noted that:

- Veterans often are driven by their support for the shared "mission" and because of their training possess strong values and ethics.
- Their military experience has provided them with years of cybersecurity experience in "live fire" scenarios, working on systems comparable to those found in the civilian work environment.
- Their network of military "buddies" makes a veteran-hire a rich resource for recruiting their friends and colleagues.
- Their veteran status means they have ongoing access to continuing education, training, and certification programs.
- Veterans may already possess (and need to maintain) desirable security clearances.
- Veterans are often from underrepresented populations in the cybersecurity industry, such as minorities, women, and persons with disabilities.

Consequently, veterans bring far more to the talent pool than mere education and training credentials.

Additionally, organizations with cybersecurity positions deal with very high turnover rates driven by the workforce shortage and competition for trained and qualified staff. Anecdotally, veterans tend to be company-loyal and less likely to job-hop, preferring to work in a team environment and commit to the shared goals of the organization. They are more likely to stay with a firm that enables them to work with their buddies and military colleagues. Workshop participants indicated that companies that invest in veteran hiring and

development will potentially be rewarded with hard-working, committed, and diverse employees.

1.4. Stages of the Military Experience – Early Service

Workshop attendees recommended that discussions of the concepts necessary for a successful transition to civilian careers become a normal and regular part of military life (i.e. career planning, skills development, resumé writing, etc.) While in the military, service members can receive cybersecurity education, develop skills, and receive funding or other support to earn industry-recognized cybersecurity certifications. Workshop participants recommended the following:

- More be done at the earliest stages of military service to present cybersecurity as a desirable and in-demand field. This may begin as early as recruitment, while in reserve officer training corps (ROTC), and in early years at military and service academies.
- Bootcamp should include a Cybersecurity 101 course. This would ensure that all military personnel become versed in general cybersecurity concepts that are important for all to know and to highlight military roles that track to civilian careers.
- Bases could offer extracurricular or outside-of-work opportunities for all military staff in cybersecurity, along the lines of a CyberPatriot-style "capture the flag" competition. Military bases could stage competitions against each other, in person, or virtually.
- Branches of military should develop and field a cybersecurity aptitude test to identify early service members who could thrive in cybersecurity careers. This aptitude test could also be offered to military spouses and adult children.
- The military can assist the veteran by tracking their military service KSAs and military occupational specialty code (MOS) using the NICE Framework to help translate military experience to civilian work. This could be a transcript that continues to build throughout their service and is available to them upon transition in online and printed form.

There is an opportunity to promote the value of gaining cybersecurity experience as well as knowledge and skills while in the military. For military roles that track closely to civilian careers, for example, cyber operations and signal corps, extra effort should be made to identify common knowledge areas or the various civilian certifications that are used in the military sector. Even for those whose military roles aren't completely technical, there are opportunities for learning while in the service that will improve transition opportunities. These opportunities might include online courses during off-duty hours.

1.5. Stages of the Military Experience – Mid-career

Workshop attendees noted that there are opportunities for active service members to continue building skills, both with military-provided training and civilian training. Existing specialty programs for active military include programs such as "Education with Industry," which is an Air Force program that is a highly selective, non-degree education program while the airman is in the force. They are matched with an industry partner in their field of interest, with a

lengthy learning and working term. Additionally, the assigned industry site may not be anywhere near an Air Force base, offering the participant a chance to live and work as a civilian, for as long as a year. The military member gains management and industry experience and acts as an ambassador for the military in the company and community they are stationed with.

Attendees also noted that information about free and subsidized training courses, online programs, webinars, and industry-recognized certifications should be readily available to service members and their families. Service members could develop affinity groups based on their work area within their military branch (across locations), use social media to promote and support ongoing education opportunities, and differentiate opportunities in cybersecurity by business operations and technical operations (helping with transition to civilian work roles). As allowed by rules of the service member's command, military leaders should encourage military personnel to engage in cybersecurity professional communities, attend industry conferences for continuing education, and offer to develop opportunities on base for fellow military personnel.

Cybersecurity courses could also be made available to military spouses and dependent children. In fact, veterans can transfer portions of their education benefits to their dependents. There are also financial support programs to assist spouses who are pursuing academic degrees and other credentials. Marketing and courses for this group may need to be handled differently from the workforce training and education efforts targeted to military personnel.

1.6. Stages of the Military Experience – Pre-Transition

Programs designed to support veterans should be offered earlier than many participants experienced. Currently, service members may not know what support is available to them, pre-transition, nor how to obtain that support. According to attendees, many do not receive support until after they have already separated. Yet, there are many programs which currently offer assistance to transitioning service members. For example, the "Vet Life" program (reportedly) works best if done before the transition phase. (Vet Life is a non-profit faith-based program, part of "Life Renewed International" aka "Operation Not Forgotten", which is primarily a volunteer-led support group.)

Examples of specialty programs that could be leveraged for the cybersecurity workforce at the pre-transition phase are SkillBridge and JTEST [9]. These are both Department of Defense (DOD) programs that help transitioning veterans find civilian training programs. These programs can begin prior to transition, and the services are provided on base. These programs could be provided specifically for cybersecurity careers.

SkillBridge is described on their website as an "opportunity for service members to gain valuable civilian work experience through specific industry training, apprenticeships, or internships during the last 180 days of service. SkillBridge connects service members with industry partners in real-world job experiences." JTEST, which stands for "Job Training, Employment Skills Training, Apprenticeships, and Internships (JTEST-AI)," helps in matching transitioning veterans to internships. It is available for "an eligible service member

(who) must complete at least 180 continuous days on active duty and is expected to be discharged or released from active duty, within 180 days of starting the JTEST-AI." With the approval of their commanding officer, the authorized service person can start a professional internship while still on active duty and ease their transition to full employment. Additionally, they act as "ambassadors" of the military to the local business community.

SkillBridge and JTEST programs may vary from location to location, or simply not exist for some military service people. Workshop participants raised concerns about this. If a service person wants a specific career opportunity such as cybersecurity, what options might exist if these programs don't provide it? Would a commanding officer be open to approving an online course or custom internship? How do we ensure there are consistent programs across the network of all military branches and locations? These programs should be provided specifically for cybersecurity careers where possible.

A concerted, industry-supported pre-transition assistance program (pre-TAP) for cybersecurity could help map the service member's career objective outside of military so they could plan training courses and certifications while in the service. Unlike current military-led transition assistance programs such as discussed later in section 1.7, the pre-TAP could begin at any stage of military service, instead of only when separation is imminent. This could aid service members separating unexpectedly due to medical issues, after their initial tour of duty, or through retirement.

The workshop participants remarked that it can be challenging for service members to compare college and university programs with community college programs, and then evaluate the need for industry-recognized certifications. The pre-TAP could depict a flexible roadmap with steps to take during their career and transition process to ensure speedy onboarding to their post-military career. In addition to civilian opportunities, the program should talk about cybersecurity career opportunities and benefits to be found in federal, state, local government, and tribal territories.

Veterans in the workshop discussed that, among their peers, civilian salaries are poorly understood; that it's hard to imagine making the leap from in-service pay to five- and six-figure salaries afterwards. They also report it's challenging to answer the typical interview question of "what sort of compensation did you have in mind?" As part of a pre-TAP preparation, salary ranges for civilian versus government positions should be included to assist military personnel with selecting desired post-military career paths and to answer this question with confidence. The NICE-supported website Cyberseek.org will be useful for showing civilian salaries in different geographic locations and for different work roles, and the government jobs site, CyberCareers.gov, is helpful for understanding federal positions.

1.7. Stages of the Military Experience – At Transition

With approximately 200 000 [10] military veterans transitioning to civilian life each year, there is potential to create strong pathways into cybersecurity careers that will benefit thousands of organizations. The primary resource to all transitioning military is the Transition Assistance Program or TAP, managed by the U.S. Department of Veteran Affairs.

It's a required program for all veterans and reserve members (with 180 days plus of active duty). TAP offers many important programs including (but not limited to):

- Transition GPS: Goals, Plans, Success (DoD)
- Counseling and individual transition planning
- Career coaching (resumé skills, how to use LinkedIn, interviewing skills)
- Career technical training track
  - Includes credentialing, help finding courses, how to locate funding
- VA Benefits I – four hours on financial, insurance, health care, etc.
- VA Benefits II – 2-hour video on using the VA Benefits portal
- Military One Source services: https://www.militaryonesource.mil/

The workshop participants stated that, as comprehensive and valuable as TAP is, the TAP program happens too late for most veterans. In response to feedback such as this, TAP is being updated and introduced earlier in the veteran's career, as much as a year before transition time. Other comments indicated that though their TAP program offered a wide variety of resources to the entire veteran population, it's not flexible enough to offer a customized experience that is tailored to cybersecurity career coaching and KSA mapping. At the time of a veteran's transition, the military has an enormous amount of general transition information to impart. For example, transitioning veterans are taught about personal finance and banking, relocation opportunities, and strategies for getting health care and life insurance.

For the specific career needs in cybersecurity, attendees suggested it might be better to separate that experience out and offer an online training course developed in partnership with industry. They recommended that a cybersecurity-specific TAP program be created and used throughout all branches of the military or customized to fit each branch's needs. The TAP Cybersecurity materials should leverage the transcript or portfolio discussed in section 1.5 and help a veteran map the work they have done, the clearances and certifications received, and their areas of interest as they pertain to civilian opportunities. Veterans need help in tracking skills and knowledge of both hardware and software, manufacturer and industry certifications, and maintaining or continuing to keep certifications up to date. Programs are needed to ensure that as a military person qualifies for a certification they are guided to sit for the exam and maintain the qualification through to transition.

One workshop participant mentioned that within Army Intelligence they have mapped roles to a career pathway leading to cybersecurity jobs. Integrating the Cyberseek.org website into the TAP program could help a service member visualize their career outside the military. And as veterans have likely never been in a formal job interview before, they should receive instructions during a TAP program on what research is normal to conduct about a target company or job description before an interview and specific to cybersecurity careers. Practice interviews should be part of the cybersecurity TAP (if it isn't already) and include preparation for discussing salary and other typical interview questions.

The transitioning veteran could be matched with an online mentor who would coach them as they go through the cybersecurity TAP program. The veterans could be provided with tools to map all their experiences in the military to civilian careers and job listings, to develop industry appropriate resumés, and to conduct practice interviews using Skype or other video chat services with their mentor.

Social media sites such as LinkedIn are presented during TAP, yet for some, this may be the first time the service members have heard of them and their use in job hunting. Using LinkedIn requires guidance and experience, and many could benefit from a longer training on its use. Veterans should be provided with training and mentoring on use of social media in their career planning. They should be instructed on how to find the many cybersecurity industry and affinity groups on LinkedIn.

1.8. Industry – Ways They Can Help

There is a great opportunity for industry to participate in a service member's transition to the civilian workforce, both pre- and post-transition. During the workshop, it was pointed out that some industry organizations are very successful in hiring and retaining veterans, while others struggle. Attendees made several recommendations for ways industry can help turn transitioning service members into successful employees.

Industries or companies with a large cybersecurity workforce might partner with and support the transition programs of branches of service and at nearby bases or posts. Such organizations can offer material to support groups, support educational opportunities, and engage with affinity and industry groups in their local areas. Convening a group to create a location-specific cybersecurity career report could be the beginning of a coordinated regional hiring effort that focuses on veterans. As materials grouped by geographic region are made available, they should be distributed to veterans from other areas who wish to relocate. The cybersecurity career location report should be online or otherwise in a shared repository so the benefit can be utilized as broadly as possible. As a veteran in any branch readies to transition, they should be able to combine their service work transcript report with the cybersecurity career location report for their desired civilian community.

Apprenticeships are increasingly being adopted for "white collar jobs" like cybersecurity. The Executive Order Expanding Apprenticeship in America specifically mentions veterans as an attractive population to participate in these programs [11, §6]. Industry could create distinct opportunities for wounded veterans (for example, through remote and working-from-home positions). Industry can provide early training for transitioning veterans by hosting courses on military bases or online with veteran or military access programs. It may be possible for apprenticeships to be conducted during the transition phase, such as in the last six months of a service member's tour of duty, assuming the location and specialty areas map to the needs of local employers.

Another concern for industry that impacts veterans is retention; the turnover of personnel in the cybersecurity field is high because competing companies offer financial incentives to change employers or because the nature of the work and shortage of staff may lead to

overwork and burnout. That doesn't appeal to a veteran desiring a team and stability. Industry should present information on the many resources they provide all employees, and specifically veterans, to demonstrate the level of support their employees receive to address workplace morale and work/life balance. For example, discuss more than salary and earning potential and emphasize the teamwork and camaraderie of the firm's cybersecurity staff. Make sure that those on the interview teams have some longevity in the company and present a unified message to the veteran candidate.

Industry could collaborate on a cybersecurity veterans guide that explains the kinds of work done in each role and related skillsets. There are some good materials in distribution from individual companies and organizations, but they lack a common language or map of military roles and skills to civilian life. Mapping to the NICE Cybersecurity Workforce Framework could resolve that in the cybersecurity realm. Employers should make sure that job listings don't create barriers for applicants, such as listing and filtering applications on job requirements that are highly restrictive, such as certifications or advanced degrees that are typically unnecessary for entry level roles. A well-written veterans guide could supplement the gaps in available in-person coaching programs that are regional or restricted in scope. Veterans need a comprehensive resource guide that provides information beyond their base or post, including virtual learning and training options. For those veterans who intend to relocate after their transition, having more geographic information would be very useful.

In cybersecurity, the notion of a career path is something that is still evolving. The Career Pathways area of the Cyberseek website can help a veteran or any job seeker understand possible pathways. But it cannot be guaranteed that someone can remain in a role or naturally progress in a planned career path. Pathways allow for decisions such as a return to higher education or time spent in related work that can be difficult to predict. A veteran might not be accustomed to this level of uncertainty about their future. Industry should create cybersecurity pathways on their career websites so a veteran (or any applicant) can see how the roles they are seeking fit into a larger corporate opportunity. Even for a smaller company, the information can be imported from Cyberseek and be used to reflect the general industry sector of which they are a part.

Understanding why industry wants and needs to hire veterans is key; but so is building support for these programs beyond the hiring manager level. Executive suite and human resources support of a veteran hiring program is crucial. It is also helpful to look for support from an organization's local and Federal-elected officials who may have developed incentive and programs for their constituency. Industry should actively seek information on veteran-hiring incentives such as tax credits, GI bill, and other federal-funding support to veteran hiring. It may be useful and necessary for the companies to report their veteran hiring data for tracking to programs with local, state or federal funding.

A civilian human resources manager may be unfamiliar with many of the issues presented when hiring veterans. The terminology used to describe work in the military varies by branch: Military Occupation Specialty code (MOS) for Army and Marines; Air Force Specialty Code (AFSC) for Air Force and Rating for Coast Guard and Navy. Materials could be developed to educate hiring managers and human resources staff on these issues. The

civilian hiring manager should become familiar with or able to map military skills and experience to the roles they seek to fill. Job descriptions should be written using clear language so that terms used to map military experience match. The same tools a veteran might use to build a resumé should be available to human resources professionals. Requirements for security clearances should be described in language that matches military clearance language.

One of the concerns raised in the workshop was that senior military personnel, such as someone with twenty years' service, may believe that they will automatically find a senior role in industry. The recruiters themselves may initially see the senior personnel as potential company leaders and ignore more junior veterans. The reality may be that the senior leaders' skills point towards a mid-career spot or their technical knowledge is of less value than they assumed. It can be devastating to take a step down, just to get into a civilian technology or cybersecurity role.

Industry should require their human resources and recruiting staff to present veteran candidates for all open positions and have ready metrics on veteran candidates and their rate of hiring. It would also be good for industry to share success stories. Prepare "day in the life" stories and videos of veterans who have successfully transitioned from each branch of the military to cybersecurity roles in civilian life. Ensure veterans are successful after they are hired by creating mentoring programs – whether mentors are veterans or not. Industry should support internal affinity groups and provide them with senior executive sponsors.

1.9. Post-Transition Challenges and Resources

Career Planning: It was frequently mentioned during the one-day workshop that it can be challenging for veterans to see how their experience or military role translates to careers. Yet, there are websites and tools designed to make this relatively simple. One method to map military role to civilian role is to use the O*Net website (onetonline.org). Caveat: roles on O*Net don't necessarily state "cybersecurity" in their titles so one should be creative in use of terms.

A search on O*Net's My Next Move for Veterans website provides information on careers in general and careers that are similar to military work. One might search on an entry-level cybersecurity role such as "information security analyst" and see results that include the role's tasks, knowledge, skills and abilities required for the position and even links to videos with more details about the career [12]. However, a search for a branch of the military and the term "*cyber,"* will return more specific information. Another example: select "*Air Force"* and enter the word "*cyber"* in the search box and the returned results will include a variety of related roles in the civilian world. Other commercial sites such as Military.com have a skills translator tool [13]. The veteran only needs to provide their branch of service and either a role by number or they can enter key words to see what real world job opportunities they may qualify for. Using websites like these could be part of the pre-transition program work and are highly useful for the veteran at any stage of their career research.

Pressure to Work: For many reasons a veteran may feel pressure to find work as soon as possible after leaving military life. They may accept the first offer of employment or even apply for jobs they are overqualified for. Their financial situation may be challenging, with debt or high costs to provide for their family's needs. They may choose to move back to their home community and want to start living independently right away. If they have debt (such as a high monthly car payment or money borrowed for housing), this may prevent them from pursuing careers that require additional education or training. Family obligations may similarly push them into the job market without enough preparation. A relocation to a community that lacks access to professional education, training or veteran programs can be a further hindrance to a transitioning veteran moving into a cybersecurity career. Veterans need support to overcome short-term difficulties that might compel them to take any job on offer versus establishing a career plan and taking necessary steps to achieve those goals.

Understanding the Civilian Hiring Process: Veterans have likely never had a job interview experience. A question about desired salary levels can make a veteran uncomfortable if they haven't prepared a response. Similarly, just being asked "what value they offer" to the organization may cause a military service person to feel unprepared. Yet these are some of the normal and uncomfortable interview experiences civilian job seekers may be more familiar with. Veterans need guidance on how to research a company in advance, how to prepare for an interview, and how to follow up afterwards.

Unlike in military life where following orders leads to promotion, civilian job finding requires very different behaviors. Veterans may simply be unaware of how complex job hunting is today. There is an opportunity to educate veterans about hidden networks and "buddy" hiring. These can both help and hurt a veteran. Veterans need to be educated on the importance of building their professional network. There are skills that could be taught to veterans about doing outreach online and in person at "meet ups" and professional organization meetings.

Even once a veteran selects a community to move to after they transition, they will continue to have challenges that are directly related to their status as a veteran. They may not understand how to jump into the local job market. They may lack a relationship with a nearby military base where veteran resources are often centered. Veterans should be coached on communities or organizations that can help them get started after a move, and to help them select locations where they might wish to move. A good organization to work with in a new location is the United Service Organizations (USO) which offers a variety of services for transitioning military and their families, and they have locations across the United States.

Challenges abound in civilian employment transitions when civilian language and social demeanor is different from what a veteran knew in the military world. They may have health challenges, whether from physical limitations or post-traumatic stress disorder (PTSD). They might need an accommodation both at work and in their housing, and not know what their rights are in the workplace or elsewhere. Industry can help veterans overcome these issues in part by acknowledging that these issues exist, by providing appropriate services and support, and recognizing the contributions their veteran employees are making.

Understanding Federal or Government Hiring: Barriers and difficulties are also present when the applicant seeks a role in the federal or local government sphere. Numerous obstacles may exist that are not always clear. For example, (as was reported in the workshop discussion), in federal hiring where veterans could be the preferred candidate, a hiring manager may refuse to fill the position unless they can hire their preferred (non-veteran) candidate. These internal disputes might cause a position to appear open, because there is no real justification for not hiring a fully qualified veteran.

Job Centers: Post transition, many veterans and their families will visit their state's job centers for assistance in finding work. For those interested in cybersecurity careers they are unlikely to find appropriate guidance in these centers unless the staff is trained, and materials are provided to highlight the career pathways in cybersecurity. Industry can partner with their state's job centers to supplement available materials (print and online) and provide informational sessions to the staff and to veterans using their services. The job centers could coach veterans about the transition to the cybersecurity culture outside the military and discuss possible bias issues that may arise (such as a belief that most veterans suffer PTSD).

GI Bill and WIOA funds: Federally available funds to benefit the GI for seeking education and training (GI Bill) and funds to incentivize industry to employ targeted populations like veterans exist and should be promoted. Jobs for Veterans State Grants (JVSG) program as authorized by the Jobs for Veterans Act is part of WIOA, the Workforce Innovation and Opportunity Act [14]. WIOA funds can be used by veterans while they are learning, with priority often given to the low-income veteran.

Certification Providers: Veterans could be offered free and low-cost certification test and practice programs. A veteran may have certifications that expire due to time spent in the service (they may have qualified when they were more junior and working in more technical work, but as they rose in the service, leading other service personnel, their technical skills may have eroded.)

Other Outreach Partners: Organizations such as the USO and their transition service RP6; the Institute for Veterans and Military Families (IVMF); Veterans Affairs and many of the nonprofit organizations present at the NICE Veterans Workshop offer national and regional programs to assist with many of the critical transition issues noted in the discussion. These organizations represent some of the leading innovations and on the ground resources as efforts are made to standardize and build programs that better meet the needs of transitioning veterans to enter cybersecurity careers. Industry will find avid partnership opportunities by reaching out to these groups and helping their veterans find rewarding cybersecurity careers.

2. Key Recommendations

The following is a summary of key recommendations made during the workshop by participants. These recommendations represent potential opportunities or ideas to explore further. They are not meant to be prescriptive nor are they advocated by NIST or the NICE Program.

2.1. Military

2.1.1. Introduce and promote awareness of cybersecurity careers.

a. Create cybersecurity 101 for all military while in basic training. Include an aptitude test to evaluate all recruits for natural abilities in cybersecurity.

b. Create competitions on base (or virtually) for military, staff, and families.

c. Create promotional materials for high schools that map a cybersecurity career that includes military experience.

d. Include information about cybersecurity careers at all phases of military life: recruiting, basic training, via base and military communications such as base newspapers, and television and radio programming.

e. Create "day in the life" and success stories campaigns that demonstrate the lucrative and meaningful cybersecurity careers for veterans.

f. Create cybersecurity career programs for military family members: spouses and older children.

2.1.2. Create a pre-TAP program with standard career and training transcript or portfolio.

a. Portfolio should be available to active duty military for comment/editing.

b. Portfolio should be included in transition preparation and used to develop resumés.

c. Advertise the many courses and certifications programs, available on base and online and at local training centers and academic institutions, that are free or low cost to active duty and veteran military.

2.1.3. Standardize TAP experience.

a. Separate career-specific transition preparation from general audience needs. Industry could assist in creating a TAP for cybersecurity professionals with much of the material delivered in an online, virtual experience

b. Assign mentors – ensure that transitioning cybersecurity veterans are matched to a veteran mentor.

2.2. Industry

2.2.1. Create a comprehensive guide.

a. Create a comprehensive guide to cybersecurity careers including common terms, certifications, and links to helpful tools and websites.

2.2.2. Create veteran career pathways and publicity/marketing.

a. Create more veteran- specific roles such as apprenticeship or trainee opportunities. Create dedicated career sections on their website for veteran hiring.

b. Write job descriptions that map to military MOS and KSAs.

c. Offer online interviewing and other supportive onboarding programs for candidates that may not be able to travel.

2.2.3. Support veterans in the workplace.

a. Support individuals with affinity groups, provide new employees with a veteran employee mentor from more seasoned hires; with housing and financial support during the hiring process; with guidance to hiring managers about special veteran needs or concerns.

b. HR could coach veterans and their managers about leadership expectations or cultural norms in civilian workplace.

Acknowledgments

Thank you to the many contributors to the workshop and to attendees from these organizations:

- Federal Government: Department of Commerce/NIST; Department of Defense: (Air Force; Air National Guard; Army; Marine Corps; Navy); Department of Homeland Security (DHS); Department of Labor (DOL); Health and Human Services (HHS); Office of Personnel Management (OPM);

- State Government: Maryland Department of Labor;

- Industry: ClearedJobs.net; Fortinet; ISC2; ManTech; Military.com; Monster.com; SANS VetSuccess Academies; SC3; SkillsSmart;

- Education: Capitol Technology University; Center for Systems Security and Information Assurance (CSSIA); Montgomery County Community College; University of Maryland Baltimore County; University of Maryland University College; University of Washington;

- Nonprofits: Federal IT Security Institute (FITSI); Hire Our Heroes; International Consortium of Minority Cybersecurity Professionals (ICMCP); NPower; NS2 Serves; Paving Access for Veterans Employment (PAVE)/Paralyzed Veterans of America; Per Scholas; Vets in Tech

Thank you to the dedicated reviewers of this document: Jim Foti, Bill Newhouse, Celia Paulsen, Rodney Petersen, Davina Pruitt-Mentle, Danielle Santos.

References

[1] (ISC)^2 Management (2019) (ISC)^2 estimates cybersecurity workforce at 2.8 million. Available at https://blog.isc2.org/isc2_blog/2019/11/isc%C2%B2-estimates-cybersecurity-workforce-at-28-million.html.

[2] Burning Glass Technologies, CompTIA, National Initiative for Cybersecurity Education (2020) CyberSeek. Available at https://www.cyberseek.org

[3] The California Community Colleges Centers of Excellence for Labor Market Research (COE) (2018) Cybersecurity: Labor Market Analysis and Statewide Survey Results from California Employers and Postsecondary Institutions. (California Governor's Office of Planning and Research, Sacramento, CA). Available at http://coeccc.net/reports/Cybersecurity_Summary_Key_Findings

[4] (ISC)^2 (2018) Women in Cybersecurity: Young, Educated and Ready to Take Charge. (ISC)² Cybersecurity Workforce Study. Available at https://www.isc2.org/Research/Women-in-Cybersecurity

[5] Reed J, Acosta-Rubio J (2018) Innovation Through Inclusion: The Multicultural Cybersecurity Workforce; An (ISC)2 Global Information Security Workforce Study. (Frost & Sullivan, Santa Clara, CA). Available at https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx

[6] Ross W, Duke E (2019) A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future. (Department of Commerce, Department of Homeland Security, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/eo_wf_report_to_potus.pd_.pdf

[7] The MITRE Corporation (2020) Military to Civilian Readiness: The Past, Present and Future of the Transition Process. Available at https://www.benefits.va.gov/transition/docs/military-to-civilian-readiness.pdf

[8] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[9] Under Secretary of Defense for Personnel and Readiness (2014) Job Training, Employment Skills Training, Apprenticeships, and Internships (JTEST-AI) for Eligible Service Members. (Department of Defense, Washington, DC), Department of Defense Instruction 1322.29. Available at https://www.dodreads.com/wp-content/uploads/2019/05/DOD-Instruction-132229p-Skillbridge.pdf

[10] Veterans Benefits Administration (2020) Your VA Transition Assistance Program (TAP). Available at https://www.benefits.va.gov/transition/tap.asp

[11] Executive Order 13801 (2017) Expanding Apprenticeships in America. (The White House, Washington, DC), DCPD-201700403, June 15, 2017. https://www.govinfo.gov/app/details/DCPD-201700403

[12] My Next Move for Veterans (2020) Information Security Analysts. (U.S. Department of Labor/Employment and Training Administration, Washington, DC), Available at https://www.mynextmove.org/vets/profile/summary/15-1122.00

[13] Military.com Network (2020) Military Skills Translator. Available at http://www.military.com/veteran-jobs/skills-translator/

[14] Workforce Innovation and Opportunity Act (WIOA), Pub. L. 113-128, 128 Stat. 1425. https://www.govinfo.gov/app/details/PLAW-113publ128

Appendix A: Informative Resources

American Corporate Partners' veterans mentoring program http://www.acp-usa.org/mentoring-program/veteran-application

Blackstone has a guide on how to set up a veteran's program. https://www.blackstone.com/careers/veterans

Career Cast list of best jobs for veterans: #2 is cybersecurity http://veteran.careercast.com/jobs-rated/2017-great-jobs-veterans

Clearedjobs.net website for jobs requiring security clearance (not all jobs are cybersecurity)

ClearedJobs.Net Blog entries on Veteran Hiring: http://blog.clearedjobs.net/?s=%22veterans%22+and+%22cybersecurity%22

Cybercareers.gov: Federal cybersecurity careers

Cyberseek.org: two tools; map of cybersecurity careers throughout the US; career pathways; www.cyberseek.org

FEDVTE: free, online training in cybersecurity for veterans https://niccs.us-cert.gov/training/veterans

Fortinet's FortiVet program https://www.fortinet.com/corporate/careers/vets.html

HireHeroes https://www.hireheroesusa.org/

Hiring Our Heroes https://hiringourheroes.org/

JP Morgan Chase Veterans Jobs Mission: https://www.veteranjobsmission.com/ Coalition of companies dedicated to hiring veterans (not just cybersecurity, all fields).

LinkedIn Veterans website: https://linkedinforgood.linkedin.com/programs/veterans

Maryland Workforce Exchange Veterans Services: search under Job Seekers for Veteran Friendly Jobs https://mwejobs.maryland.gov/vosnet/Default.aspx

Microsoft Microsoft Software and Systems Academy: Online courses, available on some military bases.

Military.com has MOS (Military Occupation Specialty) mapping. http://www.military.com/veteran-jobs/skills-translator

MITRE: https://www.mitre.org/careers/working-at-mitre/military-to-mitre (example of industry career site for veterans)

MyNextMove (sponsored by DOL and O*Net) https://www.mynextmove.org/

NICCS Portal: https://niccs.us-cert.gov/

O*Net, occupation translator tool https://www.onetonline.org/

Service to School (S2S): http://service2school.org/

United States Army Human Resources Command https://www.hrc.army.mil/ numerous career and transition resources, including records

United States Department of Homeland Security: https://www.dhs.gov/homeland-security-careers/veterans

United States Department of Labor website for any employer considering hiring from transitioning military: https://www.hirevets.gov/

United States Department of Labor Veterans' Employment and Training Office (regional offices): https://www.dol.gov/vets/aboutvets/regionaloffices/map.htm

United States Department of Labor's Veterans Apprenticeship information (for vets and employers): https://www.doleta.gov/OA/veterans.cfm

United States Department of Labor Veteran Apprenticeship https://www.apprenticeship.gov/employers/hire-veterans

United States Office of Personnel Management (OPM) Cybercareers.gov website for cybersecurity jobs in the government https://www.cybercareers.gov/job-seeker/ and https://www.fedshirevets.gov/

USAJobs.gov: https://www.usajobs.gov/Help/working-in-government/unique-hiring-paths/veterans/

United States Veterans Affairs: https://www.vets.gov/employment/

United States Veterans Affairs: https://www.benefits.va.gov/VOW/for-employers.asp

United States Veterans Affairs: https://www.dol.gov/veterans/hireaveteran/pdf/Employer-Guide-to-Hire-Veterans-June-2018.pdf

United States Veterans Affairs: "Vet Success" program for veterans transitioning to higher education https://www.benefits.va.gov/vocrehab/vsoc.asp

USAjobs.com website for finding and applying for federal jobs

Veteran Career Transition Assistance Program (example of a strong, regional transition program run by a nonprofit 501C3 in Southern California): VetCTAP (https://www.vetctap.org/)

Virginia Cyber Veterans Initiative: http://cybervets.virginia.gov/ provides veterans with access to cybersecurity training.

WIOA: Dislocated Workforce Innovation and Opportunity Act (WIOA) funds for veterans while learning.