Volume 15, Number 2 ISSN 2150-5160

Allied Academies International Conference

Las Vegas, Nevada
October 12-15, 2011

Academy of Legal, Ethical and Regulatory Issues

PROCEEDINGS

All authors execute a publication permission agreement taking sole responsibility for the information in the manuscript. The DreamCatchers Group, LLC is not responsible for the content of any individual manuscripts. Any omissions or errors are the sole responsibility of the individual authors.

The Academy of Legal, Ethical and Regulatory Issues Proceedings is owned and published by the DreamCatchers Group, LLC, PO Box 1708, Arden, NC 28704, U.S.A., (828) 507-9770. Those interested in the *Proceedings*, or communicating with the *Proceedings*, should contact the Executive Director of the Allied Academies at info@alliedacademies.org.

TABLE OF CONTENTS

VIRTUE VERSUS VICE DURING TIMES OF RECESSION: BEHAVIORAL CHANGES

Shawn M. Carraher, Indiana Wesleyan University
Ronald Weinmann, North Dakota State University

ABSTRACT

Since 2008 there has been a 71% decline in new adult content available on the web. Las Vegas has seen annual declines of over 50% in building permit requests and the official unemployment rate peaked at nearly 15% in early 2011. On-line gaming has seen 10% annual increases for the last four years second to only social networking sites that have been seeing a 43% increase - thanks in part of their inclusion of on-line gaming. On-line gambling on the other hand is shrinking by 3% per year during the same time period. Drugs: Liquor consumption has decreased from 2.75 gallons per person in 1980 to 2.31 gallons in 2007 and since then has decreased slightly (2.56 %) to 2.25 gallons. Tobacco usage is also declining 3.23% per year. Illegal drug use has declined - with the exception of marijuana usage. Cocaine has seen a decrease of 48.98%, heroin of 20.25%, marijuana an increase of 86.86%, methamphetamines a decrease of 0.47%, hallucinogens a decrease of 47.59% over the last 4 years. Regular attendance at religious services has shown a slight increase in the last 4 years going from 42 to 43%. It appears that recessions might actually lead to positive behavioral changes possibly due to a decrease in flexible spending.

REFERENCES

Buckley, M., Fedor, D., Carraher, S., Frink, D., & Marvin, D. (1997). The ethical obligation to provide recruits realistic job previews. *Journal of Managerial Issues*, 9 (4), 468-484.

Budd, J. & Carraher, S. (1998). Validation of an inventory to measure attributes of strategic management. *Psychological Reports*, 82 (3 Pt 2), 1220-1222.

Carland, J. & Carland, J. (1993). The role of personality in new venture creation. *Entrepreneurship, Innovation and Change*, 2(2), 129-141.

Carland, J & Carland, J. (1995). The case of the reluctant client. *Journal of the International Academy for Case Studies*, 1(2), 76-79.

Carland, J. & Carland, J. (1997). A model of potential entrepreneurship: Profiles and educational implications. *Journal of Small Business Strategy*, 8 (1), 1-13.

Carland, J. & Carland, J. (2003). Pawn takes queen: The strategic gameboard in entrepreneurial firms. *Academy of Strategic Management Journal*, 2, 93-104.

Carland, J. & Carland, J. (2004). Economic development: Changing the policy to support entrepreneurship. *Academy of Entrepreneurship Journal*, 10(2), 104-114.

Carland, J. & Carland, J. (2006). Eminent domain: What happens when the state takes part of your land? *The Entrepreneurial Executive*, 11, 95-113.

Carland, J.A.C., & Carland, J.W. (1991). An empirical investigation into the distinctions between male and female entrepreneurs managers. *International Small Business Journal*, 9 (3), 62-72.

Carland, J.A., Carland, J.W., & Stewart, W.H. (1996). Seeing what's not there: The enigma of entrepreneurship. *Journal of Small Business Strategy* 7 (1), 1-20.

Carland, J., Carland, J.A., & Abhy, C. (1989). An assessment of the psychological determinants of planning in small businesses. *International Small Business Journal*, 23-34.

Carland, J., Carland, J., & Carland, J. (1995). Self-actualization: The zenith of entrepreneurship. *Journal of Small Business Strategy*, 30-39.

Carland, J.W., Carland, J.A., & Hoy, F. (1992). An entrepreneurship index: An empirical validation. Babson Entrepreneurship Conference, Fontainebleau, France.

Carland, J.W., Carland, J.A., Hoy, F., & Boulton, W.R. (1988). Distinctions between entrepreneurial and small business ventures. *International Journal of Management*, 5 (1), 98-103.

Carland, J.W. III, Carland, J.W., Carland, J.A., & Pearce, J.W. (1995). Risk taking propensity among entrepreneurs, small business owners and managers. *Journal of Business and Entrepreneurship*, 7 (1), 12-23.

Carland, J.W., Hoy, F., Boulton, W.R., & Carland, J.A.C. (1984). Differentiating entrepreneurs from small business owners: A conceptualization. *Academy of Management Review*, 9 (2), 354-359.

Carland, J.W., Hoy, F., & Carland, J.A.C. (1988). Who is an entrepreneur? is the wrong question. *American Journal of Small Business*, 12 (4), 33-39.

Carraher, S.M. (1991). A validity study of the pay satisfaction questionnaire (PSQ). *Educational and Psychological Measurement*, 51, 491-495.

Carraher, S.M. (1991). On the dimensionality of the pay satisfaction questionnaire. *Psychological Reports*, 69, 887-890.

Carraher, S. (1993). Another look at the dimensionality of a learning style questionnaire. *Educational and Psychological Measurement*, 53 (2), 411-415.

Carraher, S. (1995). On the dimensionality of a learning style questionnaire. *Psychological Reports*, 77 (1), 19-23.

Carraher, S.M. (2003). The father of cross-cultural research: An interview with Geert Hofstede. *Journal of Applied Management & Entrepreneurship*, 8 (2), 97-106.

Carraher, S.M. (2005). An Examination of entrepreneurial orientation: A validation study in 68 countries in Africa, Asia, Europe, and North America. *International Journal of Family Business*, 2 (1), 95-100.

Carraher, S.M. (2006). Attitude towards benefits among SME owners in Eastern Europe: A 30-month study. *Global Business and Finance Review*, 11 (1), 41-48.

Carraher, S.M. (2008). Using E-Bay to teach global and technological entrepreneurship. *International Journal of Family Business*, 5 (1), 63-64.

Carraher, S.M. (2011). Turnover prediction using attitudes towards benefits, pay, and pay satisfaction among employees and entrepreneurs in Estonia, Latvia, & Lithuania. *Baltic Journal of Management*, 6 (1), 25-52.

Carraher, S.M., Buchanan, J.K., & Puia, G. (2010). Entrepreneurial Need for Achievement in China, Latvia, and the USA. *Baltic Journal of Management*, 5 (3), 378-396.

Carraher, S.M. & Buckley, M. R. (1996). Cognitive complexity and the perceived dimensionality of pay satisfaction. *Journal of Applied Psychology*, 81 (1), 102-109.

Carraher, S.M. & Buckley, M.R. (2008). Attitudes towards benefits and behavioral intentions and their relationship to Absenteeism, Performance, and Turnover among nurses. *Academy of Health Care Management Journal*, 4 (2), 89-109.

Carraher, S.M., Buckley, M. & Cote, J. (1999). Multitrait-multimethod information management: Global strategic analysis issues. *Global Business & Finance Review*, 4 (2), 29-36.

Carraher, S.M., Buckley, M., & Cote, J. (2000). Strategic entrepreneurialism in analysis: Global problems in research. *Global Business & Finance Review*, 5 (2), 77-86.

Carraher, S.M., Buckley, M., Scott., C., Parnell, J., & Carraher, C. (2002). Customer service selection in a global entrepreneurial information services organization. *Journal of Applied Management and Entrepreneurship*, 7 (2), 45-55.

Carraher, S.M. & Carraher, C. (1996). ISO environmental management standards: ISO 14,000. *Polymer News*, 21, 167-169.

Carraher, S.M. & Carraher, C. (1996). ISO 9000. *Polymer News*, 21, 21-24.

Carraher, S.M. & Carraher, S.C. (2006). Human resource issues among SME's in Eastern Europe: A 30 month study in Belarus, Poland, and Ukraine. *International Journal of Entrepreneurship*. 10, 97-108.

Carraher, S.M., Carraher, S.C., & Mintu-Wimsatt, A. (2005). Customer service management in Western and Central Europe: A concurrent validation strategy in entrepreneurial financial information services organizations. *Journal of Business Strategies*, 22, 41-54.

Carraher, S.M., Carraher, S.C., & Whitely, W. (2003). Global entrepreneurship, income, and work norms: A seven country study. *Academy of Entrepreneurship Journal*, 9, 31-42.

Carraher, S.M., Hart, D., & Carraher, C. (2003). Attitudes towards benefits among entrepreneurial employees. *Personnel Review*, 32 (6), 683-693.

Carraher, S.M., Gibson, J. W., & Buckley, M.R. (2006). Compensation satisfaction in the Baltics and the USA. *Baltic Journal of Management*, 1 (1), 7-23.

Carraher, S.M., Mendoza, J, Buckley, M, Schoenfeldt, L & Carraher, C. (1998). Validation of an instrument to measure service orientation. *Journal of Quality Management*, 3, 211-224.

Carraher, S.M. & Michael, K. (1999). An examination of the dimensionality of the Vengeance Scale in an entrepreneurial multinational organization. *Psychological Reports*, 85 (2), 687-688.

Carraher, S.M. & Parnell, J. (2008). Customer service during peak (in season) and non-peak (off season) times: A multi-country (Austria, Switzerland, United Kingdom and United States) examination of entrepreneurial tourist focused core personnel. *International Journal of Entrepreneurship*, 12, 39-56.

Carraher, S.M., Parnell, J., Carraher, S.C., Carraher, C., & Sullivan, S. (2006). Customer service, entrepreneurial orientation, and performance: A study in health care organizations in Hong Kong, Italy, New Zealand, the United Kingdom, and the USA. *Journal of Applied Management & Entrepreneurship*, 11 (4), 33-48.

Carraher, S.M., Parnell, J., & Spillan, J. (2009). Customer service-orientation of small retail business owners in Austria, the Czech Republic, Hungary, Latvia, Slovakia, and Slovenia. *Baltic Journal of Management*, 4 (3), 251-268.

Carraher, S.M. & Paridon, T. (2008/2009). Entrepreneurship journal rankings across the discipline. *Journal of Small Business Strategy*, 19 (2), 89-98.

Carraher, S.M., Scott, C., & Carraher, S.C. (2004). A comparison of polychronicity levels among small business owners and non business owners in the U.S., China, Ukraine, Poland, Hungary, Bulgaria, and Mexico. *International Journal of Family Business*, 1 (1), 97-101.

Carraher, S.M. & Sullivan, S. (2003). Employees' contributions to quality: An examination of the Service Orientation Index within entrepreneurial organizations. *Global Business & Finance Review*, 8 (1) 103-110.

Carraher, S.M., Sullivan, S. & Carraher, S.C. (2005). An examination of the stress experience by entrepreneurial expatriate health care professionals working in Benin, Bolivia, Burkina Faso, Ethiopia, Ghana, Niger, Nigeria, Paraguay, South Africa, and Zambia. *International Journal of Entrepreneurship*, 9 , 45-66.

Carraher, S.M., Sullivan, S.E., & Crocitto, M. (2008). Mentoring across global boundaries: An empirical examination of home- and host-country mentors on expatriate career outcomes. *Journal of International Business Studies*, 39 (8), 1310-1326.

Carraher, S.M. & Welsh, D.H.B. (2009). *Global Entrepreneurship*. Dubuque, IA: Kendall Hunt Publishing.

Carraher, S.M. & Whitely, W.T. (1998). Motivations for work and their influence on pay across six countries. *Global Business and Finance Review*, 3, 49-56.

Carraher, S.M., Yuyuenyongwatana, R., Sadler, T., & Baird, T. (2009). Polychronicity, leadership, and language influences among European nurses: Social differences in accounting and finances, *International Journal of Family Business*, 6 (1), 35-43.

Chait, H., Carraher, S.M., & Buckley, M. (2000). Measuring service orientation with biodata. *Journal of Managerial Issues*, 12, 109-120.

Crocitto, M., Sullivan, S.E. & Carraher, S.M. (2005). Global mentoring as a means of career development and knowledge creation: A learning based framework and agenda for future research. *Career Development International*, 10 (6/7), 522-535.

Deng, F.J., Huang, L.Y., Carraher, S.M., & Duan, J. (2009). International expansion of family firms: An integrative framework using Taiwanese manufacturers. *Academy of Entrepreneurship Journal*, 15 (1), 25-42.

Hart, D. & Carraher, S. (1995). The development of an instrument to measure attitudes towards benefits. *Educational and Psychological Measurement*, 55 (3), 498-502.

Huang, L.Y. & Carraher, S. (2004). How effective are expatriate management and guanxi networks: Evidence from Chinese Industries. *International Journal of Family Business*, 1 (1), 1-23 .

Lester, D., Parnell, J.A. & Carraher, S.M. (2010). Assessing the desktop manager. *Journal of Management Development*, 29 (3), 246-264.

Lockwood, F., Teasley, R., Carland, J.A.C., & Carland, J.W. (2006). An examination of the power of the dark side of entrepreneurship. *International Journal of Family Business*, 3, 1-20.

Paridon, T. & Carraher, S.M. (2009). Entrepreneurial marketing: Customer shopping value and patronage behavior. *Journal of Applied Management & Entrepreneurship*, 14 (2), 3-28.

Paridon, T., Carraher, S.M., & Carraher, S.C. (2006). The income effect in personal shopping value, consumer self-confidence, and information sharing (word of mouth communication) research. *Academy of Marketing Studies Journal*, 10 (2), 107-124.

Parnell, J. & Carraher, S. (2003). The Management Education by Internet Readiness (MEBIR) scale: Developing a scale to assess one's propensity for Internet-mediated management education. *Journal of Management Education*, 27, 431-446.

Scarpello, V. & Carraher, S. M. (2008). Are pay satisfaction and pay fairness the same construct? A cross country examination among the self-employed in Latvia, Germany, the U.K., and the U.S.A. *Baltic Journal of Management*, 3 (1), 23-39.

Sethi, V. & Carraher, S.M. (1993). Developing measures for assessing the organizational impact of information technology: A comment on Mahmood & Soon's paper. *Decision Science*, 24, 867-877.

Stewart, W., Watson, W., Carland, J.C., & Carland, J.W. (1999). A proclivity for entrepreneurship: A comparison of entrepreneurs, small business owners, and corporate managers. *Journal of Business Venturing*, 14, 189-214.

Sturman, M.C. & Carraher, S.M. (2007). Using a Random-effects model to test differing conceptualizations of multidimensional constructs. *Organizational Research Methods*, 10 (1), 108-135.

Sullivan, S.E., Forret, M., Carraher, S.M., & Mainiero, L. (2009). Using the kaleidoscope career model to examine generational differences in work attitudes. *Career Development International*, 14 (3), 284-302.

Welsh, D. & Carraher, S.M. (2011). *Case Studies in Global Entrepreneurship*. Kendall Hunt P.

Williams, M.L., Brower, H.H., Ford, L.R., Williams, L.J., & Carraher, S.M. (2008). A comprehensive model and measure of compensation satisfaction. *Journal of Occupational and Organizational Psychology*, 81 (4), 639-668.

THE EFFECTS OF U.S. GOVERNMENT SECURITY REGULATIONS ON THE CYBERSECURITY PROFESSIONAL

Aleta Wilson, University of Maryland University College
Clay Wilson, University of Maryland University College

ABSTRACT

There is a shortage of cybersecurity professionals that is affecting the ability of the United States to fulfil the mandate of the Comprehensive National Cybersecurity Initiative. The purpose of this research is to find solutions to remove the barriers related to security clearance regulations that affect the cybersecurity professional. A fully qualified cybersecurity professional with the ability to obtain a clearance, may be unable to obtain a cybersecurity job because they lack the necessary clearance to apply for a job. A review of several studies and government reports confirmed the shortage of workers and security clearance processing, but none of those studies addressed the problem of the security clearance barriers. It would behoove the federal government to 1) allow students in the final semester of their cybersecurity degree program to begin the clearance investigation for a secret clearance; and/or 2) partner with industry to establish a scholarship program for students designed to develop cybersecurity professionals for government contractors. Each of these options represent a win-win for all parties and is a major step towards accomplishing what President Obama has declared as a national security priority.

INTRODUCTION

This research spotlights barriers and suggests solutions to reduce the roadblocks to solving what Obama (2009) declared to be “one of the most serious economic and national security challenges we face as a nation”—cyber security. As reported in Cyber In-security (Partnership for Public Service & Booze Allen, 2009), there are “shortages of highly skilled cyber security professionals in government, and an absence of coordinated leadership on cyber security workforce issues, despite ongoing efforts by the CIO Council, individual agencies and others.” These shortages are exacerbated by barriers related to obtaining security clearances.

As with all problems, there are multiple factors that need to be addressed which include education, cyber skills, security clearance reciprocity, and a cumbersome recruitment process in government (Partnership for Public Service & Booze Allen, 2009). Even if all the other problems were solved, the "need to know" requirement to obtain a security clearance sets restrictions on when a candidate can apply for a clearance. This research focuses on the effects of security policies on the cybersecurity professional; effects on human resource management; and, the effects on the educational system.

SCOPE

This study explores activities required to employ cyber security workers for the federal government and its contractor community. These two workforce sectors comprise an estimated 500,000 workers who must undergo a significant background check to gain employment in cybersecurity positions which are labelled as "national security positions". Those positions are defined as "activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States" (Code of Federal Regulations Title 5, Pt. 732.102).

DEFINITION OF A CYBERSECURITY PROFESSIONAL

Before one can understand the problem, it is first necessary to define a cybersecurity professional. The term is freely used while no one has a clear definition. The rapid evolution of technology is racing ahead of our federal human resource classification systems. Even the Occupational Outlook Handbook put out by the U.S. Bureau of Labor Statistics (BLS), does not contain a definition for cybersecurity professionals (U.S. Department of Labor [DOL], 2010-2011).

Some Handbook categories acknowledge positions that involve people who "plan, coordinate, and maintain an organization's information security" and ("database administrators also must plan and coordinate security measures with network administrators", and network engineers "may ... address information security issues" DOL 2010-2011). It appears the Handbook is slowly evolving to now include security in various labor categories.

Department of Homeland Security (DHS) Secretary Janet Napolitano defines Cybersecurity professionals as employees responsible for "... cyber risk and strategic analysis; cyber incident response; vulnerability detection and assessment; intelligence and investigation; and network and systems engineering" (Krebs, 2009). Frost & Sullivan conducted a survey of 10,413 information security professionals (Ayoub, 2011), which indirectly defined security professionals as those "employed as Information Security professionals and those who had cyber security as their primary job function.

The Department of Defense (DOD) usually takes the lead in defining elements related to cyberspace and cybersecurity, but as recently as May, 2011, the DOD's definitions related to cyberspace operations remain unclear. "DOD has defined some key cyber-related terms but it has not yet fully identified the specific types of operations and program elements that are associated with full-spectrum cyberspace operations" (U.S. General Accountability Office [GAO], 2011b).

The cybersecurity workforce addressed in this report consists of professionals who have information security as a major part of their job; those who self-identify as cyber or security specialists; and, those who build and maintain the national critical infrastructure of the computer systems on which the public and private sectors have come to rely.

SHORTAGE OF CYBERSECURITY PROFESSIONALS

The DHS gave Secretary Janet Napolitano hiring authority to staff up to 1,000 positions over three years, and the recently established Cyber Command with responsibility for overseeing government efforts to protect the military's computer networks, will be competing with DHS for cyber staff (CyberCommand, 2009; Krebs, 2009).

According to a Washington Post article, Alan Paller, director of research at the SANS Institute, a cyber security research and training group based in Bethesda, Md., said "[t]he NSA is already stealing every human being from the other side, so there is no space for [DHS] to hire" (Krebs, 2009). This competition for staff does not even include industry that is desperately seeking to staff their corporate needs and those of their government clients.

In 2008, the President acknowledged in a Presidential Directive that "... there are not enough cybersecurity experts within the Federal Government or private sector to implement the [Comprehensive National Cybersecurity Initiative], nor is there an adequately established Federal cybersecurity career field" (Obama, 2009).

The "federal government's cybersecurity workforce is broken, facing a serious shortage of trained personnel, an over-reliance on contractors and a hiring process that doesn't attract the right candidates", according to a new report from the non-profit Partnership for Public Service (2009). In addition to the apparent shortage, many CIOs and CISOs complain about the lack of skilled candidates that apply for federal cybersecurity jobs.

The Partnership also found problems with the scholarship programs designed to attract students to federal cybersecurity jobs. One program, Scholarship for Service (SFS), graduates about 120 students each year — but it needs to generate 500 to 1,000 graduates per year to meet the government's needs (Carlstrom, 2009). The SFS program pays full tuition plus a stipend and students must work for a federal agency for a time period equal to the length of the scholarship.

CLEARANCE POLICIES AND PROCEDURES

Some level of personnel security check is required for every government position whether a direct government employee or an indirect employee through a contractor. Since the federal government employs over 2 million people, there is a lot of turnover generated due to retirements and natural movement from job to job. Added to that is the need to investigate and/or renew clearances for contractors as old contracts end and new ones begin. All of this results in approximately 900,000 clearance cases annually (DOD, EOP, OPM, & DNI, 2010).

Clearance policies and procedures have a direct effect on the cybersecurity workforce because most cybersecurity jobs fall under the heading of National Security Positions and therefore a security clearance is required. The scope of the clearance investigation varies depending on the nature of the position, location of the position, and the degree of harm that an individual in that position can cause (U.S. Office of Personnel Management, 2002).

The process for obtaining a security clearance involves an extensive background investigation that expands based upon the potential level of harm an employee can inflict and sometimes requires that the potential hire take a polygraph test.

Delays

The security clearance process does not start until there is a "need to know", which is a fundamental tenet of security clearance regulations. Essentially, it means an individual does not need a security clearance until they are hired to perform work involving national security information. This is the crux of the regulatory problem or the chicken and the egg, because individuals cannot be cleared until they have a job requiring access, but they cannot get a job until they have a clearance. Additionally the potential hire is not submitted for a clearance investigation until late in the process. In other words, the potential hire, the educational institution, and the government have expended resources obtaining the necessary cybersecurity credentials, but the potential hire is not even submitted for an investigation until after receipt of a job offer and suitability is determined. If it turns out that the potential hire cannot pass the investigation, then even more time and resources are expended to fill the vacancy because the cycle must be restarted with another candidate.

The clearance process is almost identical for government employees and contractor employees with some variations based upon individual agency rules. In the case of government contractors, the "hiring agency" is a contractor (or non-governmental organization) and the organization must have a federal government contract that requires cleared personnel. The contractor requesting the clearance must have a "facility clearance (FCL)".

One of the main differences between the federal government employees and private sector contractors is that some contracts require contractor employees be cleared *before starting work* on the contract. This is important because, according to William Dougan, president of the National Federation of Federal Employees, the contractor workforce is approximately 5 times the size of the government employee workforce (Dugan, 2011), which is an indication that the government contractor community is more directly affected by security clearances processes than government agencies.

This inability to start work prior to receipt of a clearance is a major distinction between government and contractors, because in addition to lost productivity, government contractors lose money for every day that a vacancy remains empty. Large companies such as Lockheed Martin and Boeing, can afford to hire cybersecurity employees and pay them to do other work while awaiting their clearance. The industry term for this is "sitting on the bench". Another method used by large firms, is to issue contingency offer letters to employees, and then submit them for a clearance under one of their cleared contracts, which is called "parking". Neither of these options are available for small government contractors, which is an unintended consequence of government solicitation terms and the clearance process.

Reciprocity

OPM handles 90% of all government security clearances, but some of the intelligence agencies such as CIA, DIA, FBI, NGA, NRO, NSA, and DoS conduct their own investigations (DOD, et al., 2010). Director of National Intelligence, Mike McConnell, has been trying to make security clearances uniform and interchangeable among the intelligence agencies, and that is finally becoming a reality as one of the goals of the Security and Suitability Reform Efforts is to require reciprocity (DOD et al., 2010

The clearance procedures themselves are pretty straight forward, and the government has attempted to mitigate the problem of wasting time and resources on an in-depth investigation by having the Hiring Agency do a preliminary review of employee background documentation as a first screen for suitability. Once the Hiring Agency makes the determination that a potential hire is suitable, then they request a clearance investigation.

The amount of time it will take to obtain a decision on the suitability of the candidate based upon a background investigation varies, but the Performance Accountability Council has established a goal of 74 days for end-to-end processing of clearances (DOD, et al, 2010). If, at the end of the investigation, the candidate is rejected, then the Hiring Agency must begin the hiring process all over again with a new candidate. These rejections can increase the duration of the vacancy at a time when the country is desperate for cybersecurity professionals.

Effects of the Security Policies on Cybersecurity Professionals

There is a direct relationship between the level of clearance (i.e., Secret versus Top Secret), and the amount of time it takes to conduct a background investigation. All of this directly effects human resource management, the government contractor community, and educational institutions providing cybersecurity degrees.

Many of the current cyber jobs will become vacant over the next 10 years as half of the defense workforce becomes eligible to retire. Marion Blakey, Chief Executive Officer of the Aerospace Industries Association says the cybersecurity workforce must be home-grown because only U.S. citizens are eligible for security clearances and there are more than 7,000 job openings "many of them on defense projects and hard to fill" (King, 2010).

All of this is great news for employees with clearances because they are in high demand, which also leads to higher salaries. According to one popular website, Intelligence.com, only 2 percent of job seekers with clearances are unemployed (Wellner, 2004). Booze Allen stockpiles its supply of cleared workers by recruiting college interns, and after conducting a suitability investigation, they submit them to the security-clearance process as soon as it has a start date for the 20 to 25 staff who will work on their national security projects. Assuming the interns return when they graduate, Booze Allen has trained and cleared employees ready to go (Wellner, 2004).

Effects of Security Policies on Human Resource Management

The human resource (HR) problem occurs when the government or a contractor needs to fill a cybersecurity position. Potential cybersecurity employees are given a contingency offer letter and they may have to wait anywhere from 11 days to 71 days. About 85% of clearance requests are for Confidential or Secret clearances while the rest are for Top Secret clearances, which take approximately 65% longer than Confidential and Secret clearances. Therefore, cybersecurity professionals who frequently need Top Secret clearances will skew toward the higher end of investigation times.

The government contractor has an additional HR problem associated with government contract bids, because many government solicitations require cleared personnel be submitted with the bid. Therefore, a company may not be able to bid on a contract because they lack cleared personnel who are already on staff. This barrier means that a company with the best cyber expertise but lacking a facility clearance and no "cleared" cybersecurity professionals may not be able to bid.

Effects of Security Policies on Educational System

The US government has put several programs in place to increase the supply of cybersecurity professionals through education. These programs have placed increased emphasis on education in science, technology, engineering, and math (STEM) resulting in a public-private partnership with over $260M to be invested over the next decade (Obama, 2009). This mandate is being compared to the investment the United States made in engineering for the "race to the moon", during the Kennedy administration. In fact, growth in STEM jobs was three times as fast as growth in non-STEM jobs during the last 10 years (2011). Unfortunately, the results of STEM investment may not begin to surface for another ten years, and may not help the cyber workforce problem at all.

Another effort targeting university level education is being addressed through Center's of Academic Excellence outreach efforts designed and operated by the National Security Agency (NSA), and the Clinton Administration's Policy on Critical Infrastructure Protection (CIP) (Clinton, 1998; National Security Agency, 2010b). The CIP program goal is to reduce vulnerability in our National Information Infrastructure by promoting higher education in information assurance (IA), and to produce a growing number of professionals with IA expertise in various disciplines.

As of 2010, there were one hundred twenty-four (124) National Center's of Excellence certified by the National Security Agency, Central Security Service (NSA, 2010a). These institutions offer both cybersecurity degrees and certificate programs and the length of each program varies depending on the offering institution.

Neither the STEM initiatives, National Center's of Academic Excellence, or scholarships can produce the cybersecurity talent that is needed now (Partnership for Public Service & Booze Allen, 2009). At the end of the day, a person may have the requisite STEM background and university credentials, but may not be able to obtain a security clearance unless they are "parked" or "sitting on the bench" at a large government contractor company.

CONCLUSION

Since the demand for cybersecurity professionals is a national security priority, it would behoove the federal government to modify the security regulations specific to cybersecurity professionals so they can begin their clearance investigation prior to having a "need to know". This would eliminate the waste and inefficiency associated with "parking" and "sitting on the bench", and would enable small businesses to offer their highly skilled cybersecurity professionals for clearances. The investigation process should begin while in their last semester of school.

Since the Center's of Excellence are approved by the National Security Agency, it seems feasible that the government would go one step further and grant facility clearances to the 124 Centers. This would allow the university or college to submit students in the cybersecurity related programs for a secret clearance during their last semester. If the suitability and clearance investigation occurs in parallel with the last semester, then the student will complete their education and obtain the clearance concurrently. This will make the student immediately available for cybersecurity employment.

Considering the value of a clearance to the employee, and since a clearance investigation costs the government money, the government should require a work commitment from the student of at least two years in exchange for the clearance. A side benefit is that the government would have a level of predictability regarding the cybersecurity workforce pipeline.

A second option is for Center's of Excellence to develop Memorandums of Understandings (MOUs) with industry partners that have FCL's. The industry partner would agree to hire the students during their final semester either full-time, part-time or as an intern and begin their clearance investigation. Like the first option, the student would agree to work for the company for a specified period of time.

Third, since contractor employees outnumber government employees five-to-one, the federal government should partner with industry to create a Scholarship for Service Program designed to develop cyber professionals for government contractors. Each of these options represent a win-win for all parties and is the final link in the chain for implementing the Comprehensive National Cybersecurity Initiative.

Further research on this topic might include exploring the effect of security clearance barriers on small businesses that sell IT services to the government. Also, should investigate whether company's with the best cybersecurity skill sets and staff are being eliminated from competing for government contracts due to a lack of security clearances.

REFERENCES

Ayoub, R. (2011). The 2011 (ISC)2 Global Information Security Workforce Study. In ISC2 (Ed.), (pp. 1-26): Frost & Sullivan. Retrieved from https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC%20Study_020811_MLW_Web.pdf

Carlstrom, G. (2009, July 22). Too few in pipeline for cybersecurity jobs, CIOs complain. *Federal Times*. Retrieved from http://www.federaltimes.com/article/20090722/IT01/907220302/-1/RSS

Clinton, B. (1998). Presidential Decision Directive/NSC-63, Retrieved from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

CyberCommand. (2009). U.S. Cyber Command Fact Sheet

DOD, EOP, OPM, & DNI. (2010). Security and Suitability Reform Strategic Framework (pp. 37). Retrieved from http://lastpostpublishing.com/Documents/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf

Dugan, W. (2011). The dollars and sense of rightsizing the federal workforce June. Retrieved from http://federaldaily.com/articles/2011/06/20/comment-william-dougan-federal-workforce.aspx

King, R. (2010). Boeing Enlists Hollywood to Make Engineering Cool. [Article]. *BusinessWeek.com*. Retrieved from *http://www.businessweek.com/technology/content/aug2010/tc2010082_406649.htm*

Krebs, B. (2009). DHS Seeking 1,000 Cyber Security Experts. *Washington Post* [Blog]. Washington, DC.

National Security Agency. (2009). Information Assurance, Centers of Academic Excellence Retrieved July 22, 2011, 2011

National Security Agency. (2010a). Centers of Academic Excellence Retrieved May 28, 2011, 2011. Retrieved from http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

National Security Agency. (2010b, September 10, 2010). National Centers of Academic Excellence Retrieved from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

Obama, B. (2009). The Comprehensive National Cybersecurity Initiative Retrieved from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Partnership for Public Service & Booze Allen. (2009). Cyber In-security: Strengthening the Federal Cybersecurity Workforce. Washington: Partnership for Public Service and Booze, Allen, & Hamilton. Retrieved from www.ourpublicservice.org/OPS/publications/download.php?id=135

U.S. Department of Labor. (2010-2011). *Occupational Outlook Handbook, 2010-2011 Edition, Bulletin 2800* (2010-2011, Bulletin 2800 ed.). Washington, DC: U.S. Government Printing Office, Washington, DC, 2006.

U.S. General Accountability office. (2011b). Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates (pp. 33). Washington, DC: General Accountability Office.

OPM. (2002). General questions and answers about OPM background investigations Retrieved June 4, 2011, 2011, from http://www.opm.gov/products_and_services/investigations/faqs.asp

Wellner, A. S. (2004, March, 2004). The hunt for candidates with defense agency security clearances. *Workforce Management, 83,* 80-82.