Congressional Hispanic Caucus Institute, Inc.
CHCI

CHCI White Paper

DEVELOPING THE NEXT GENERATION OF LATINO LEADERS®

April 2016

Securing Our Nation: Diversifying the Federal Cybersecurity Workforce Pipeline

By Amber T. Seira, *CHCI-Motorola STEM Graduate Fellow*

Executive Summary

In recent years, the United States witnessed information cyber attacks on private corporations like Chase and Target as well as public sector entities like the U.S. Office of Personnel Management (OPM). While many strategies to develop technological innovations for counteracting cyber attacks exist, no investment is arguably more influential than the employee talent pool. The rate and complexity of cyber threats demand an equally multifaceted workforce to outsmart growing technology security issues. Implementation of H.R. 2952 and S. 1691 from the 113th Congress initiated restructuring of our federal cybersecurity workforce; however, more cohesive, inclusive legislation is necessary to bolster the diversity of talent. Furthermore, as more Latinos obtain technology credentials and reach workforce age, their labor participation in the technology sector is proportionally underrepresented. The skilled workforce essentially excludes Latinos from careers with greater job security and higher wages. As a component to its overall workforce pipeline and retention strategy, federal agencies should be held accountable to leverage Latino talent to fill its cybersecurity workforce needs.

This white paper provides context for both the nation's and federal government's workforce participation of Latinos. Furthermore, this paper identifies technology workforce management gaps, which hamper improvement of technology security among federal agencies. This analysis concludes that temporary new talent initiatives such as 18F, the federal agency consultant group, or Information Technology (IT) contract procurement will not sustain a viable workforce. While securing all aspects of technology labor vulnerabilities proves important, the momentum in Congress is in strong support of securing cybersecurity policy. Therefore, tangible cultural shifts in stabilizing the technology workforce should retool approaches in cybersecurity education, recruitment, and retention with the intention of investing in strategy, rather than financial resources, to diversify the early to mid-career professionals of the cybersecurity workforce pipeline. Policy recommendations in this paper involve strategies focused on new codification of cybersecurity workforce standards, reorganizing existing education training efforts, supplementing current cybersecurity workforce legislation, and soliciting updated workforce research as a result of revised strategy goals.

Policy Background

Diversification of the federal cybersecurity workforce pipeline intersects in three areas—Latino education and workforce participation, demographic aspects of federal cybersecurity laborers, and existing laws governing cybersecurity. While Latinos display increased levels of education attainment, (*Excelencia*, 2015) they are not benefiting from high-skilled careers. Furthermore, talent deficits exist in the federal cybersecurity workforce. Lastly, the 113th Congress supported acts to invest and better manage the cybersecurity federal workforce, alluding to the political feasibility in bolstering federal cybersecurity. Understanding the nuanced backgrounds of these three areas indicates paths for possible policy solutions.

Latinos And Technology Careers

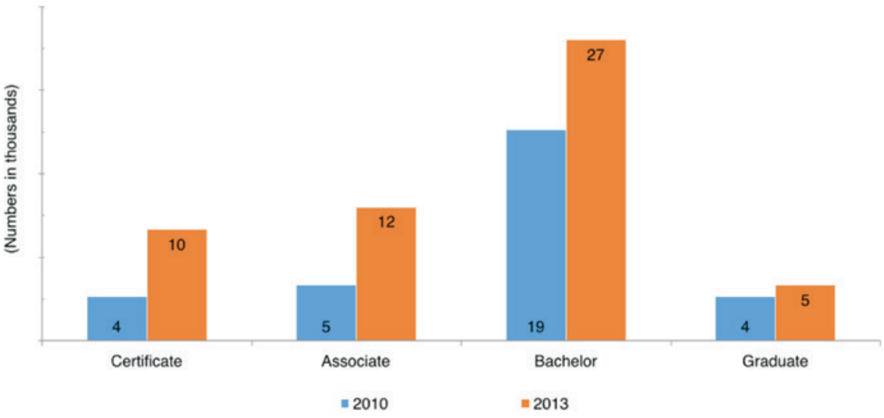
In the last decade, more and more students are filling up the front end of the Science Technology Engineering and Math (STEM) pipeline. Between 2010 and 2013, the credentials earned by Latinos in STEM have increased by 74 percent, according to a study by *Excelencia* in Education (2015). This research further describes that in the 2012-13 school year alone, approximately 50 percent of Latinos graduating in STEM fields earned bachelor degrees (2015). More specifically to the technology sector, Hispanic graduates in 2014 represent 7.7 percent of all total bachelor degrees awarded in disciplines computer science, computer engineering, information systems, information technology, and software engineering (Zweben and Bizot, 2015). The increased number of degrees attained by Latino students portrays the rising Latino workforce and a snap shot of those who are trained to enter the nation's much needed careers.

Unfortunately, more credentialed Latinos does not directly translate into populating

The opinions expressed in this paper are solely those of the authors and do not represent or reflect those of the Congressional Hispanic Caucus Institute (CHCI).

“Hispanic employees also only account for 10 percent of federal employees aged 33 and younger (OPM, 2014). “

Figure 1: Latinos have increased credentials in STEM



Source: *Excelencia* in Education analysis of NCES, IPEDS, 2009–10 and 2012–13 completions surveys.

private sector tech jobs. Weise and Guynn determined that, “only half of Black and Hispanic graduates with computer science degrees from leading universities are being hired by major technology companies” (2014). Comparatively, three-quarters of white graduates with computer science degrees are being hired by major technology companies (Weise and Guynn, 2014). The mean annual wage in computer and mathematical jobs was $80,180 in 2012 (DOL, 2012), yet Latino and African Americans often experience higher instances of unemployment or underemployment, forcing them to exit the higher-paying tech sector (Excelencia, 2015). Facilitation of STEM educated individuals must grow beyond education pipelines and paired into long-lasting careers.

Federal IT Employment and Latinos

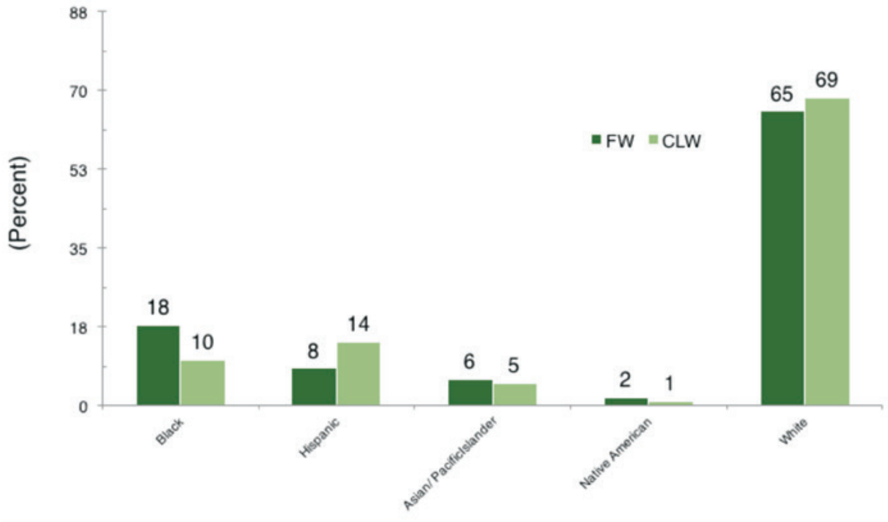
Federal agencies face a deficit of IT employees where investment in early career maturation is an immediate workforce need. In regards to federal technology employees, there are now “nearly 11 times more federal IT workers aged 50 or above than there are IT employees under the age of 30 — up from nine times more just two years earlier” (Kash, 2013). As the 2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) survey determined, the average cybersecurity employee is above the age of 40. The inability to recruit and retain younger employees into the cyber workforce pipeline hinders an agency’s ability to maintain a sustainable workforce.

Latino employment representation is also dismal across the federal agencies and even more so across technology career positions. In the fiscal year 2012, Hispanic overall employment represented merely 8.2 percent federal workforce whereas Hispanic employment composed 14.2 percent of the civilian workforce (FEORP). In comparison, Figure 2 shows White employee percentages make up 65.4 percent of the federal workforce and 68.5 percent of the civilian workforce (FEORP, 2013). Hispanic employees also only account for 10 percent of federal employees aged 33 and younger (OPM, 2014). While part of the gap in Hispanic employment can be attributed to citizenship requirements for certain government positions, when corrected for this factor, a representative imbalance of Latinos in the federal sector not reflective of the nation’s population still exists.

Latino employees are also underrepresented in technology occupations of the federal government sector despite the growing amount of credentialed Latinos in STEM fields. More specifically to technology employees, the number of new Hispanics on-board in the permanent federal workforce by the computer science occupation was 3.5 percent of government-wide new hires in Fiscal Year 2012 (OPM, 2013). Latino representation is about 5 percent of the total 2210 workforce series, the most common series for cybersecurity professionals, whereas White federal employees account for approximately 65 percent of personnel in the same workforce series (FedScope, 2014). This low representation proves disappointing as the importance of a diverse workforce goes beyond philosophical representation. Research shows that “companies that rank in the top quartile for racial and ethnic diversity are 35 percent more likely to have financial returns above their respective national industry medians” (Hunt, Layton, & Prince, 2015). The lack of Latino representation in federal technology employment supports the need for purposeful measures to increase cybersecurity diversity which, in turn, may enhance transnational competitiveness. Securing a technology system proves important because it requires a combination of innovative tools for preventing, monitoring, and mitigating possible cyber attacks, from hackers domestic or abroad.

> ***"Congress is overall supportive for federal cybersecurity needs, with over 20 bills introduced in the 114th Congress alone. The most recently passed cybersecurity legislation is the Cybersecurity Act of 2015, with minimal workforce provisions located in Division N of the Omnibus Act. "***

Figure 2: Comparison of Permanent Federal Workforce and Total Civilian Labor Force (September 2012)



Source: Federal Equal Opportunity Recruitment Program (FEORP) for Fiscal Year 2012. U.S. Office of Personnel

Cybersecurity Workforce Legislation
Congressional federal technology oversight is typically cautious of passing structurally demanding laws. Past legislative efforts have historically placed federal IT human resources responsibilities onto the Chief Information Officers (CIO) across all federal agencies through measures such as the Clinger Cohen Act (1991) and E-Government Act of (2002). Existing legislation codifies responsibilities for strategizing, assessing, hiring, and managing IT workforce talent. Legislation specific to the cybersecurity workforce typically delegate specific procedures to the U.S. Department of Homeland Security (DHS). All of these efforts lack specific language to encourage diversity recruitment or retention.

The current Congress is overall supportive for federal cybersecurity needs, with over 20 bills introduced in the 114th Congress to date. The most recently passed cybersecurity legislation is the Cybersecurity Act of 2015, with minimal workforce provisions located in Division N of the omnibus Act. Three bills passed in the 113th Congress focus on bolstering the DHS workforce. As shown in Figure 3, public law 113–246 and 277 codified for DHS to assess, strategize, retain and train their cybersecurity workforce as well as provide additional funding to DHS for hiring and compensation to assess workforce needs, yet these Acts lack provisions cognizant of talent diversification.

Cybersecurity workforce legislation 113-274 pertains to cybersecurity education pipeline needs by reauthorizing financial resources for the National Science Foundation to maintain their CyberCorps Scholarship for Service Program. The CyberCorps scholarship provides a stipend covering tuition and expenses for students. In exchange, graduates must work in a Federal, State, Local, or Tribal Government organization in an information assurance position equivalent to the time length of the stipend. A criticism of this initiative suggests that the scope of the program's participating institutions list is limited from where majority of diverse cohorts earn their postsecondary credentials. When considering Latino STEM credential completion, approximately 2 percent of all postsecondary institutions graduate 33 percent or more of their Latino students (*Excelencia*, 2015).

Figure 3: Cybersecurity legislation during 113th Congress

Public Law	Title	Cybersecurity Workforce Focus
113-246	Cybersecurity Workforce Assessment Act	Requires an assessment by DHS of its cybersecurity workforce, develop a workforce strategy
113-277	Border Patrol Agent Pay Reform Act of 2014	Provides additional DHS hiring and compensation authorities, requires a DHS assessment of workforce needs
113-274	Cybersecurity Enhancement Act of 2014	Provides statutory authority for an existing NSF cybersecurity scholarship and recruitment program

Source: Fischer, E. (2015, April 29). Cybersecurity Issues and Challenges: In Brief. Washington, D.C.: Congressional Research Service.

“They address key talent acquisition methods combining short-term obligations with project subject matter flexibility, a growing strategy employers use to attract adult millennial, born between 1980 and 1996, tech hires (Ernst & Wyborny, 2014).”

Contracting as a Labor Tool

Arguably not every cybersecurity-related role necessarily needs to exist in-house. While contracting IT services is a common approach to fill talent gaps, this strategy impairs the growth of sustaining the cybersecurity sector. Typically, the federal government pays “contractors 1.83 times more than the government pays federal employees in total compensation for comparable services” (Project of Government Oversight, 2011). Specific highly-skilled positions that will be obsolete within two or three years should not require the investment in new hires or staff training, but rather function within other labor tools such as short-term contracts. This strategy proves particularly critical within cybersecurity functionalities as certain activities, such as monitoring techniques, may be phased out within two years by newer security innovations. A better solution would be to hire permanent staffers who are more broadly skilled and can therefore fulfill several federal workforce needs. This solution will help sustain the career lifecycle of permanent federal employees, making them a more valuable long-term asset than temporary, contract positions.

Alternatively, Federal Communications Commission CIO David Bray argues that strong internal staff development is needed as a way to strengthen federal IT capabilities. Bray cites how mitigation of increased IT contracts still requires permanent staff with IT knowledge to properly procure services (Bray, 2015). Essentially little capacity exists at federal agencies to use contracts for technology acquisition because there are not enough employees with technology skill sets to oversee the contract of services. Ultimately, Bray argues for favoring bottom-up managerial approaches that innovate from within the workforce (Bray, 2015). The goal here lies in cultivating people to become the best and the brightest in the organization as agents of change, having preexisting and new hires working side-by-side.

Special Federal Hiring Strategies

Federal agency leaders recognize talent vulnerabilities and have responded with short-term solutions to fulfill immediate workforce needs. The U.S. Digital Services (USDS) team and 18F are two federal government initiatives with the intention to spur rapid, home-grown technology innovation. USDS provides tech project management whereas 18F operates as in-house development team, yet both efforts exist as an internal consulting tool. USDS Administrator Mikey Dickerson pitches the experience where staffers join “not as bureaucratic lifers but volunteers, working for intense bursts” (Levy, 2015). Essentially, new employees enter into temporary positions for up to two years on a limited salary under these tech consulting programs.

The benefit of 18F and USDS initiatives provides a direct approach for fostering federal IT innovation with younger and newer talent. They address key talent acquisition methods combining short-term obligations with project subject matter flexibility, a growing strategy employers use to attract adult millennial, born between 1980 and 1996, tech hires (Ernst & Wyborny, 2014). 18F and USDS are also cost-saving programs. The Federal Times reports that such initiatives saved the General Services Administration about $150 million by taking a “more technically informed approach to procurement” (Boyd, 2015). The notion of agile workgroups prompted the U.S. Department of Defense to create a similar model with the focus on cybersecurity entitled Defense Digital Services. While this approach yields higher diversity applicant hiring, such methods for all three initiatives lack language for ensuring intentional strategies to incorporate diversity talent acquisition, especially among Latinos.

The aforementioned remedies still ignore long-term pathways to engaging younger, more diverse federal employees in career federal technology jobs. Using a combination of special hiring authorities or strategically leveraging workforce series and position descriptions operates within rather than against the labor cultural preferences of the millennial cohort. Ultimately hiring trends such as USDS and 18F yields the end goal of effective product innovation. Strategies which revitalize workforce talent and address contract cost savings must also contain realistic sustainability measures to ensure innovation maturity however, when special hiring strategies lack measures for permanent positions within career federal roles then it makes this new talent method potentially vulnerable to last the lifespan of a single administration.

Policy Criteria

One way of measuring policy recommendations lies in measuring how well they align with the following criterion: political feasibility, federal implementation, equitability, and budgetary impact. The categories are defined by the following capacities. Political feasibility examines the most recent behaviors of Congress and forecasts how actionable a recommendation can reasonably occur. Federal implementation acknowledges recently developed frameworks and determines how likely a proposed policy adoption can sensibly occur. Equitability distinguishes

> ***"In lieu of creating new legislation, some policy solutions could restructure current legislative offerings. For instance, the CyberCorps Scholarship for Service Program needs to widen its talent pools by recruiting at additional institutions where diverse talents are in larger quantities. "***

Figure 4: Policy evaluation category table.

Policy Criteria	Ideal Policy	Importance
Budgetary Impact	Minimal Allocation	Highest Priority
Federal Implementation	Aligns Well	Mid-Level Priority
Equity	Directly Influences	Priority
Political Feasibility	High	Priority

how influential the recommendation applies to fostering diverse talent. Budgetary impact examines the extent in which a proposal will require additional financial resources. As depicted in Figure 4, the ideal policy recommendation will have high political feasibility, aligns well with federal initiatives, and directly influences diverse talent while minimizing financial resource allocation. As policy recommendations are reviewed in the next section, these criteria will be applied to each one to determine its potential success.

Policy Recommendations

Policy recommendations to bolster the federal cybersecurity workforce pipeline must balance both strengthening legislation and maintaining federal agency agility. Starting points for workforce reform include (1) new codification of cybersecurity workforce standards, (2) reorganization of existing education training efforts, (3) supplementation of current cybersecurity workforce legislation, and (4) solicitation of updated workforce research due to revised strategy goals. All recommendations encourage policy restructuring where intentional diversity can promote better inclusion of Latinos in the federal cybersecurity workforce.

Codifying Workforce Standards

Congress should codify cybersecurity workforce standards in accordance with the National Initiative for Cybersecurity Education (NICE) framework as a means to create a foundation for agency leadership to adhere to cybersecurity pipeline efforts and positively influence diversity recruitment. The comprehensive NICE framework outlines 31 functional work specialties within the cybersecurity field and provides a common language in regards to professional cybersecurity work types and categories. This framework can serve as a powerful tool for realigning efforts across federal agencies and creating a sophisticated cybersecurity workforce pipeline. Legislation should ensure minimum benchmarks set forth by the NICE framework so that all stakeholders, from aspiring students to hiring managers, can benefit from predictable workforce expectations. Moreover, the framework should further include a section requiring CIOs and their leadership teams to establish diversity strategy standards for the hiring and recruitment process.

Previously, Congress enacted laws requiring for development of the NICE framework, but its implementation among federal agencies is inconsistent and serves as a reference guide at best. The aim for codifying the NICE framework lies in improving the strength and uniform implementation of cybersecurity workforce standards. A benefit to this approach is that Congress is setting a baseline of quality rather than overreaching agencies workforce decisions.

Legislating cybersecurity workforce standards would have moderate political feasibility as it would be challenging to create and pass new technology acts. For instance, current information-sharing legislation recently passed both House and Senate chambers, but it takes time. Information sharing initiatives began in the 112th Congress but it's the 114th Congress that is presenting a final bill to the president.

Federal agencies would be able to implement this recommendation and experience less disruptive transition issues because it builds from a preexisting framework developed to guide federal agencies. Creating legislation from the framework would make standardizing the cybersecurity workforce no longer an opt-in choice by technology or agency leadership. Codifying baseline hiring standards would not impede, but rather support, agencies in shoring up strategy plan implementation. This recommendation does not directly combat Latino inequity issues; however, it would attempt to set a standard for diverse hiring or recruitment models where CIOs are forced to contemplate and formalize a more conscious approach. Finally, the financial investment for each agency to respond to such legislation would depend on the degree in which technology leadership is already implementing the framework. Some agencies may or may not need additional staff hires to assess and implement the standards.

Expanding Cybercorps Scholarship Program

In lieu of creating new legislation, some policy solutions could restructure current legislative offerings. For instance, the CyberCorps Scholarship for Service Pro-

“Policy recommendations in this paper involve four strategies: new codification of cybersecurity workforce standards, reorganizing existing education training efforts, supplementing current cybersecurity workforce legislation, and soliciting updated workforce research as a result of revised strategy goals.”

gram needs to widen its talent pools by recruiting at additional institutions where diverse talents are in larger quantities. Of the 61 CyberCorps participating institutions, only one is located at a Historically Black College and University (HBCU) and none are located at a Tribal College. Furthermore, there are only nine participating institutions who meet the enrollment definition as a Hispanic Serving Institution (HSI) and only one campus is a top institution graduating Latinos in STEM degrees, thus meeting the 33 percent Latino graduated threshold. Therefore, the CyberCorps scholarship legislation should mandate program availability to more students studying at Hispanic Serving Institutions (HSIs), Historically Black Colleges & Universities (HBCUs), and and Tribal Colleges to represent a minimum 25 percent of CyberCorps participating institutions.

This recommendation aims to readjust education pipeline approaches supporting currently articulated strategic goals as it applies bullet point 2.4 from the National Initiative for Cybersecurity Education (NICE) Strategic Plan for Cybersecurity Education, which encourages supporting students studying cybersecurity from diverse backgrounds. Thus, adjusting the CyberCorps scholarship program complements current federal initiatives and should have a low impact for administration implementation. Adjusting aspects of the CyberCorps scholarship program directly counteracts Latino equity pipeline issues. Political feasibility is high as it the scholarship program bill, 113–246, already passed Congress before. Lastly, not only did 113–246 pass the scholarship program, but it also appropriated funds for it, implying that this solution could remain a priority within the budget.

Legislation Amendments

Congress should also consider adding components to current cybersecurity legislation that targets fostering competitive and diverse talent. Enhancing legislation such as 113–274 or 113–277 should include language for intentional diversity competitiveness for attracting younger and Latino talent, such as student loan repayment for new cybersecurity hires who are members of a traditionally underserved group. Legislative language also needs to reinforce congressional oversights aimed to address securing diversity in cybersecurity workforce infrastructure. This recommendation differs from previously mentioned policy recommendation because it focuses on adjusting preexisting legislation.

The aim of this policy recommendation focuses on refining existing workforce laws by being intentional about inclusivity. By focusing on laws that have successfully passed Congress, additional clauses about diversity might be able to pass more easily through current the legislative process. This recommendation directly addresses Latino equity and may have moderate to high political feasibility. Furthermore, adjusting the language of current law may have low to no impact to current budget appropriation levels as long as no additional resources are proposed in the amendments. Depending on the current culture and adaptive nature of an agency’s cybersecurity workforce priorities, this proposal might have moderate difficulty for agency implementation. However, requiring agencies to be cyber secure and diversity aware at the same time minimizes any silo effects of diversity-only legislation because it forces agency leadership to critically strategize simultaneously.

Federal Workforce Updated Study

The Information Technology Workforce Assessment for Cybersecurity (ITWAC) 2012 study intended to collect workforce data to help distinguish the federal civilian cybersecurity workforce proficiency and composition; however, the 2012 report lacked emphasis in diversity demographics. This study was conducted in partnership with the Federal Chief Information Officer’s Council and NICE. This recommendation will provide crucial updates to Congress of cybersecurity workforce developments as well as specifically address workforce demographics in detail.

Ultimately, Congress should require updated information as a method to hold transparency and accountability among agencies. With new cybersecurity workforce initiatives, such as re-segmenting the federal cybersecurity occupation code, the proposed survey should be able to differentiate labor information of that personnel overhaul. Lastly, placing research efforts on measuring diversity is also communicates to agencies that workforce priorities explicitly involve talent inclusivity.

This recommendation has high political feasibility, as Congress is invested in its oversight responsibilities and provides an equity outlet for congressional intervention. It is unknown how favorable Congress would be toward allocating financial resources for the study, but if it granted the ITWAC 2012 survey, it should still be viewed positively. Lastly, federal agency implementation should not be too difficult as the 2012 study could be replicated in terms of project sponsorship, coordination, and research has already happened.

Cybersecurity is an immediate national threat in need of infrastructure overhaul, and while the Latino community makes up significant portions of the rising 21st century workforce, it remains underrepresented in the federal civilian workforce.

Conclusion

Solving the Federal IT workforce deficiencies needs to also proactively address Latino employment underrepresentation. Cybersecurity rises as an immediate national threat in need of infrastructure overhaul, and while the Latino community makes up significant portions of the rising 21st century workforce, it remains underrepresented in the federal civilian workforce. Policy recommendations in this paper involve four strategies: (1) new codification of cybersecurity workforce standards, (2) reorganizing existing education training efforts, (3) supplementing current cybersecurity workforce legislation, and (4) soliciting updated workforce research as a result of revised strategy goals. Codifying federal cybersecurity workforce standards and expanding the CyberCorps scholarship program are the more achievable recommendations to execute, according to the defined policy criteria. Both initiatives could be championed through the legislative process, while citing specific language for diversity inclusiveness. Given its recent political feasibility, Congress and federal agency leadership have the momentum to begin moving the needle for a sustainable, inclusive workforce that embraces technology innovation and Latino talent.

Works Cited

Boyd, A. (2015, September 9). "DoD 'Force of the Future' includes Civilian Digital Services team." Federal Times.

Bray, D. (2015, September 17). Public Panel. "Stewards of the Public Trust: Closing the Gaps in Federal Cyber Infrastructure." Association for Federal Information Resources Management.

Bray, D. (2015, October 11). "Why Cultivating Bottom-Up Change Agents Trumps Top-Down 'Command and Control'." Web log. LinkedIn Pulse. linkedin.com/pulse/

Bureau of Labor Statistics. (2011). Current Population Survey. Table 39. U.S. Department of Labor. bls.gov/cps/cpsaat39.htm/

DPE Research Department. (2014, March). The STEM Workforce: An Occupational Overview. Fact Sheet 2014. Washington, D.C.: Department for Professional Employees.

Ernst, R. & Wyborny, T. (2014). Hiring Millennials: The Generation that Changes Everything. Genisis10. Online PDF. genesis.10.com/wp-content/

Excelencia in Education. (2015). Finding Your Workforce: Latinos in Science, Technology, Engineering, and Math (STEM). Washington, D.C.: Excelencia in Education.

FedScope, Federal Human Resources Data. (2014). FedScope Employment Data Cubes: Employment. Washington, D.C.: U.S. Office of Personnel Management.

Fischer, E. (2015, April 29). Cybersecurity Issues and Challenges: In Brief. Congressional Research Services. Washington, D.C.: Congressional Research Services.

Hunt, V., Layton, D., & Prince, S. (2015, February 2). Diversity Matters. United States: McKinsey & Company.

Kash, W. (2013, September 24). "Federal IT Staffing Mess: Budget Chaos + Aging Workforce." Information Week Government Special Report.

Levy, S. (2015, July 30). "Stock Options? Don't Need 'Em! I'm Coding for Uncle Sam!" Backchannel, Medium Corp.

National Initiative for Cybersecurity Education. (2013, March 14). 2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) survey. Washington, D.C.: Federal CIO Council.

Project of Government Oversight. (2011). Bad Business: Billions of Taxpayer Dollars Wasted on Hiring Contractors. POGO.

United State Office of Personnel Management. (2013). Federal Equal Opportunity Recruitment Program (FEORP) for Fiscal Year 2012. Washington, D.C.: U.S. Office of Personnel Management.

United State Office of Personnel Management. (2014). Federal Employee Viewpoint Survey Results: Employees Influencing Change. Washington, D.C.: U.S. Office of Personnel Management.

United State Office of Personnel Management. (2013). Twelfth Annual Report to the President on Hispanic Employment in the Federal Government. Washington, D.C.: U.S. Office of Personnel Management.

Weise, E. and Guynn, J. (2014, October 13) "Tech jobs: Minorities have degrees, but don't get hired." USAToday.

Zweben, S. and Bizot, B. (May 2015). "2014 Taulbee Survey." Table B7. Computing Research News. Vol. 27 No. 5. Online PDF. cra.org/resources/crn-online/