50 YEARS
MARYLAND
Chamber of Commerce
FOUNDATION

Where we are – Cybersecurity & Information Technology (IT)

There are more jobs available than candidates. Think about this. A field where the unemployment rate is zero and the expansion of this sector seems infinite. While the future of this sector is indeed endless, there are workforce development and talent pipeline issues to be addressed. Among them is the difficulty in finding talent, which we believe are attributed to two major factors – security clearances and job classification, especially in the public sector. We break down these two topics, and conclude with a third on preparing the next generation of cyber and IT talent.

We made these briefs because we want policymakers, business leaders and the community to understand, at a high level, the issues at hand in order to equip themselves as they work to create a brighter future for all Marylanders.

Security clearances

History

Although the apparatus for restricting the dissemination of restricted information has been around since before the Romans, the modern security clearance model got its start post World War II with the National Security Act of 1947. This was also the time that the Cold War began and spy-craft proliferated. The need for protecting secrets became even more important.

Fast forward 50 years, the first major reform of security clearances in the new millennium was through the Intelligence Reform and Terrorism Prevention Act of 2004. One of the major products of this Act was making it mandatory for agencies to accept security clearances from other agencies. Although this provision went into effect, it has not been fully adopted partly because agencies are allowed to add security clearance requirements which slows the transfer between agencies.

Additionally, due to Congressional concerns over the backlog of security clearances - which was previously being handled by the U.S. Department of Defense (DoD) - Congress included a provision in the Defense Authorization Act of Fiscal Year 2004, which transferred many of the background checks to the Office of Personnel Management (OPM).[1] [2]

Major Events

Three major incidents helped shape the current conversation concerning security clearances:

1. The Washington Navy Yard Shooting (September 16, 2013) – during this event, a contractor entered the Washington Navy Yard and killed 12 people, marking the incident as the second deadliest on a U.S. military instillation. The importance of this event was the report by now-Chief of Naval Operations Admiral John Richardson, who lead the

[1] https://www.opm.gov/news/releases/2004/11/opm-consolidates-bulk-of-federal-security-clearance-process-with-transfer-of-over-1800-employees-from-defense-department/

[2] https://federalnewsradio.com/opm/2017/11/why-opm-is-warning-against-dod-reclaiming-the-security-clearance-process/

Navy investigation. This report found, among other issues, that the background check of the perpetrator of the shooting was not thorough as it did not find important information from his past. Additionally, the report noted that more people are given access to classified information than necessary.[3] It is almost as supervisors are checking a box off a form requiring a certain level of clearance for certain positions.

2. US Investigation Services (USIS) Cyber Attack (July 2014) – a major contractor running background checks for OPM – USIS – was hit by a cyber-attack, crippling its ability continue with OPM and DHS issue stop-work orders. When this contractor, who was screening 21,000 security clearance cases a month, was up for its contract renewal with OPM in September 2014, OPM decided not to renew. Because of USIS's hack and the subsequent cancellation of their contract with OPM, hundreds of thousands of security clearances were delayed.[4]
3. OPM Data Breach (announced June 2015) – OPM announced in June 2015 that it had suffered a major data breach in mid-2014 that made more than 21 million records vulnerable, including those individuals who had gone through background checks. These attacks occurred in mid-2014 and although they did not cause or make worse the security clearance backlog, they hurt the reputation of OPM and arguably caused the full-circle we see now as Congress is moving security clearances back to DoD – the opposite of what it did in 2004.

History

For almost 15 years, the National Background Investigation's Bureau (NBIB) (formerly the Federal Investigative Service, NBIB post-2016) at OPM handled almost 95 percent of background investigations for federal employees and contractors requiring security clearances.[5] Although DoD and other agencies (including the Central Intelligence Agency) partly run their own background investigations, the vast amount of investigations were handled by NBIB.

As of March 2018, NBIB had 710,000 pending cases, with 530,000 of those being classified as backlogged.[6] This number had not been confirmed for some time, but recent federal legislation has made these figures and other statistics public.

Similar to the mood in 2003-2004 when Congress became frustrated with DoD's background check abilities, Congress was irritated with OPM for a multitude of reasons and transferred – under the National Defense Authorization Act (NDAA) for Fiscal Year 2017 – background checks for all DoD employees. This process would not need to be completed until FY2019 as the Secretary of Defense can waive certain deadlines until then.[7] It has been speculated that the

[3] http://archive.defense.gov/pubs/Navy-Investigation-into-the-WNY-Shooting_final-report.pdf

[4] https://www.washingtonpost.com/business/economy/opm-to-end-usis-contracts-for-background-security-checks/2014/09/09/4fcd490a-3880-11e4-9c9f-ebb47272e40e_story.html

[5] https://nbib.opm.gov/about-us/

[6] https://www.gao.gov/products/GAO-18-431T - Through Public Law No: 115-173 – SECRET Act – the reporting on this background will be made public.

[7] https://www.militarytimes.com/news/pentagon-congress/2018/06/03/pentagon-to-take-over-security-clearance-checks/

DoD's Defense Security Services (DDS) will be responsible for background checks and take the process fully out of the hands of OPM.

For the past year, policymakers, business leaders, contractors and the public are waiting for and wondering when an Executive Order will come out of the White House to resolve this question.[8]

History often repeats itself. To think that 15 years ago Congress was making the same judgements over the delay in security clearances and transferred responsibility from DoD to OPM and that the opposite will soon be happening, makes many believe that the security clearance transfer is not meaningful reform.

Some believe more staff at appropriate agencies would be helpful. We agree that more money for staff would be helpful, but believe this should be a last resort. Innovative and efficient programs should be examined thoroughly first. Additionally, we see the multitude of continuing resolutions to fund the government and lack of meaningful procurement and contracting reform as hindering impactful progress to the overall security clearance effort.

<u>Associates degrees and matching education with jobs</u>

For decades the mantra had been every student needs a four-year college degree. Now, we are starting to realize that not everyone needs one and more importantly, many exciting careers can be attained with an associate's degree or certificate. This is very true in the cybersecurity field, where technical and industry-certified experience are often better than four-year degrees. However, as we have seen, this does not always happen in practice.

With the creation of the National Initiative for Cybersecurity Education (NICE) based on the recommendations of President Obama's Cyberspace Policy Review, NICE, and its parent organization, the National Institute for Standards and Technology (NIST), have been working diligently to address issues that hamstring the development and proliferation of a cyber-workforce.[9] In November 2017, NISTIR 8193 (Draft) – NICE Work Role Capability Indicators – was created to help human resources teams and managers across the federal government to reevaluate their current educational, work-related employment, and hiring criteria to make sure that eligible candidates are not left out for disqualifiers such as an educational degree.

NICE and NIST are working with departments and agencies across the federal government to make sure that the knowledge, skills and abilities that are required for cyber-related roles are correct. Currently there is a degree of non-symmetry among cyber and IT related jobs among departments and agencies and a lack of guidance, which has led many human resources managers to incorrectly classify certain jobs. These incorrect classifications are most notable when we look at minimum education requirement.

[8] https://federalnewsradio.com/reorganization/2018/08/trump-administration-preparing-executive-order-to-transfer-security-clearance-program/

[9] https://fas.org/irp/eprint/cyber-review.pdf

While most cyber-security related positions on the General Service scale do not have minimum requirements for education, not all human resources teams and hiring managers know this. Because these individuals, who often write the applications that are advertised online, do not know many of these positions do not have minimum education requirements and that work experience can substitute many of the requirements, they submit jobs requisitions in which they put a bachelor's degree as the minimum requirement even though it is not necessary. Additionally, even when human resources teams know that there is no minimum education requirement for the position, they often do not question the hiring manager. [10]

The good news is that NICE is aware of this problem and is working diligently to correct it. We are confident that this will be resolved.

This is especially important to Maryland as we host a number of National Security Agency (NSA) and Department of Homeland Security (DHS) certified Centers of Academic Excellence. These institutions include College of Southern Maryland, Anne Arundel Community College, University of Maryland University College and 13 others in Maryland. They are all certified by NSA and DHS as providing up to date cyber education that have direct applications in the federal workforce for cyber defense and operations.

Next generation of cyber talent

Maryland is fortunate to have many educational options that allow students to explore and become proficient in cybersecurity and IT. These options allow students to gain academic and professional experience to take on jobs in these and related fields.

Maryland Public School Education

The Maryland State Department of Education as part of the Career and Technology Education program hosts a Homeland Security and Emergency Preparedness program of study as one of their Human Resource Services Clusters.

Students going through this CTE program earn industry certification and college credit for:

- Homeland Security Science
- Criminal Justice and Law Enforcement
- Information/Community Technology

Internships

Currently the state internship program that helps technology-oriented interns is the Maryland Technology Internship Program. This program was expanded during the 2018 Legislative Session to allow businesses with more than 150 employees to participate in this program and use the reimbursement that it comes with.

[10] https://csrc.nist.gov/CSRC/media/Publications/nistir/8193/draft/documents/nistir8193-draft.pdf

We know that employers hiring for entry-level positions want bright students who have strong workforce experience on their resumes – making internships crucial. The number of internships available are far fewer than the number of students interested in interning, which is why we support tax credits (intern tax credits) to incentivize businesses to take on interns as being good for business, good for students and a good approach to proliferating internships.

Sparking interest and preparing early (including avoiding disqualifiers)

The Governor's Workforce Development Board Task Force of Cybersecurity and Information Technology's *Computer Science Education and Professional Development Findings Report* (June 2018) presents an excellent set of recommendations for how to improve educational attainment and workforce development in the cyber and IT sectors. Their recommendations are as follows[11]:

- Host and promote computer science public events
- Recognize formal and informal pathways to computer science careers
- Increase mentorship and coaching opportunities for youth
- Increase access to computer science courses
- Grow computer science participation and interest among women and minorities
- Develop a tech extension partnership program
- Create a Maryland computer science fellowship program
- Increase awareness among parents and students of the United States Government security clearance process

After a year with these recommendations on the books, it is important that we are following them.

[11] http://www.gwdb.maryland.gov/pub/gwdbcompscirep.pdf