SECURITY CLEARANCES: CLEARING THE PATH TO MORE JOB OPPORTUNITIES
Acknowledgements

The Partnership thanks Zaynab Malik for her research, writing and management of this issue brief. This report benefited greatly from the insights and expertise of several contributors:

MIKE BRUNI
TALENT ACQUISITION OFFICER, U.S. FEDERAL GOVERNMENT

MOE ELNABAWI
NATIONAL PRACTICE DIRECTOR, GOVERNMENT SERVICES, APEX SYSTEMS

PENNY CANTWELL
VICE PRESIDENT, SANDY SPRING BANK AND BOARD MEMBER OF FORT MEADE ALLIANCE

TOM KIRCHMAIER
SENIOR VICE PRESIDENT FOR PLANNING, COMMUNICATIONS, AND TRADE COMPLIANCE, GENERAL DYNAMICS

CLAY MCNERNEY
PRACTICE DIRECTOR, INTELLIGENCE SECTOR DELIVERY, APEX SYSTEMS

TIM O’FERRALL
PRINCIPAL, THE O’FERRALL GROUP AND GENERAL MANAGER OF FORT MEADE ALLIANCE

BONNIE ZUCKERMAN
MANAGER, APPRENTICESHIPS, NORTHROP GRUMMAN

Although these individuals reviewed the report, neither they nor their organizations necessarily endorse its findings or conclusions.
INTRODUCTION

Though the Capital Region has a deep and diverse digital tech workforce, the region will not reach its full economic potential if its digital tech and security clearance jobs are left unfilled.

The U.S. federal government has a large economic footprint in the Capital Region—spanning Baltimore to Richmond—spending approximately $152 billion in FY2018 and providing over 430,000 federal jobs. Many of these jobs require access to national security classified information, which means that these employees need to have security clearances. Individuals working for federal contractors may need security clearances as they also handle classified information on behalf of the government.

With such a large government presence, Capital Region employers hire more workers with a security clearance than employers in any other region in the United States. Job postings in the region that ask for security clearances represent approximately 9 percent of all job postings, with 50 percent of those postings representing digital tech jobs. Security clearances are by far the most highly requested credential for individuals working in digital tech.

There has been a considerable slowdown in security clearance processing time—with current processing time averages ranging from 221 to more than a year (depending on the type of clearance). Given the Capital Region's disproportionate share of jobs requiring a security clearance, the backlog in applications has an outsized impact on the region's competitiveness. Given the unique staffing needs of the Capital Region, it is no surprise that there is great competition within and between the government and private sector for top talent with security clearances. Though the Capital Region has a deep and diverse digital tech workforce, the region will not reach its full economic potential if its digital tech and security clearance jobs are left unfilled.
FIGURE 1: SECURITY CLEARANCE CATEGORIES

TOP SECRET
Information that reasonably could be expected to cause exceptionally grave damage to the national security if disclosed to unauthorized sources. Reinvestigated every 5 years.

SECRET
Information that reasonably could be expected to cause serious damage to the national security if disclosed to unauthorized sources. Reinvestigated every 10 years.

CONFIDENTIAL
Information that reasonably could be expected to cause damage to the national security if disclosed to unauthorized sources. Most military personnel are given this basic level of clearance. Reinvestigated every 15 years.

Any employee with access to national security classified information must possess a security clearance. A broad range of jobs in almost every industry require a security clearance, with most of these jobs in the federal government and authorized federal contractors. This includes professions across various industries, from intelligence analysts at the FBI to registered nurses working in the executive branch to linguists working for federal contractors in the private sector.  

There are three main types of security clearances: confidential, secret, and top secret. Figure 1 outlines the security clearance system in greater detail.

There is an additional, yet unofficial, clearance category not included in Figure 1. This category is Top Secret/Sensitive Compartmentalized Information (SCI). This category is often referred to as being “above” a Top Secret clearance. An example of information that falls in this category is the president’s daily briefing.

There are also three statuses of security clearances:

1. **ACTIVE** – Present job requires use of a security clearance.
2. **CURRENT** – Had a job in the past two years that required use of a clearance.
3. **EXPIRED** – More than two years since an individual had a job that required a clearance.

“Current” security clearances are in high demand from employers as they are fairly easy to reinstate. Reactivating expired clearances is more difficult.

From a worker perspective, security clearances offer both increased job prospects and opportunities for higher pay. Jobs requiring a security clearance can pay thousands of dollars more than counterpart positions that do not require a clearance. According to a survey conducted by ClearanceJobs.com, security-cleared candidates earn an average of 22 percent more than their non-cleared counterparts.
The Capital Region is the top hiring region in the United States for workers with security clearances. In 2018 alone, there were over 115,000 jobs requesting a security clearance available to the public via online postings (note: there may be duplicates in these figures as multiple contractors bidding for the same contract may post for the same job). Figure 2 shows the top 10 metropolitan areas in terms of the total number of job postings with a security clearance requirement. Two of the three metropolitan areas in the Capital Region make the top 10; the Washington metropolitan area is the clear leader in job postings with a security clearance requirement, followed by the Baltimore metropolitan area in the number two position.

Figure 3 visualizes which employers most frequently requested security clearances in their job postings in 2018. The federal government and government contractors were the standout requestors of security clearances.

Within each of the employers in Figure 3, there is a range of occupations requiring security clearances.

Figure 4 shows that most of these occupations are in the IT and engineering space, and that workers such as administrative assistants and technical writers can require security clearances as well.

Data from job postings demonstrate the spectrum of positions individuals can access with the help of a security clearance. From the sheer number of postings to the diverse number of employers and positions open, having a security clearance in the Capital Region is a clear asset.
## FIGURE 2: TOP METRO AREAS WITH SECURITY CLEARANCE REQUIREMENTS IN JOB POSTINGS

<table>
<thead>
<tr>
<th>RANK</th>
<th>METRO AREA*</th>
<th>JOB POSTINGS</th>
<th>JOB POSTINGS PER 10,000 PEOPLE EMPLOYED, LAST 12 MONTHS</th>
<th>LOCATION QUOTIENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Washington-Arlington-Alexandria, DC-VA-MD-WV**</td>
<td>102,485</td>
<td>340</td>
<td>Much higher demand than average</td>
</tr>
<tr>
<td>2</td>
<td>Baltimore-Columbia-Towson, MD**</td>
<td>16,413</td>
<td>127</td>
<td>Much higher demand than average</td>
</tr>
<tr>
<td>3</td>
<td>Los Angeles-Long Beach-Anaheim, CA</td>
<td>15,662</td>
<td>27</td>
<td>Average demand</td>
</tr>
<tr>
<td>4</td>
<td>Virginia Beach-Norfolk-Newport News, VA-NC</td>
<td>15,545</td>
<td>214</td>
<td>Much higher demand than average</td>
</tr>
<tr>
<td>5</td>
<td>San Diego-Carlsbad, CA</td>
<td>14,197</td>
<td>104</td>
<td>Much higher demand than average</td>
</tr>
<tr>
<td>6</td>
<td>Huntsville, AL</td>
<td>13,621</td>
<td>655</td>
<td>Much higher demand than average</td>
</tr>
<tr>
<td>7</td>
<td>Dallas-Fort Worth-Arlington, TX</td>
<td>8,656</td>
<td>26</td>
<td>Lower demand than average</td>
</tr>
<tr>
<td>8</td>
<td>Boston-Cambridge-Nashua, MA-NH (Metropolitan NECTA)</td>
<td>8,548</td>
<td>34</td>
<td>Average demand</td>
</tr>
<tr>
<td>9</td>
<td>San Antonio-New Braunfels, TX</td>
<td>7,978</td>
<td>84</td>
<td>Much higher demand than average</td>
</tr>
<tr>
<td>10</td>
<td>Colorado Springs, CO</td>
<td>7,763</td>
<td>296</td>
<td>Much higher demand than average</td>
</tr>
<tr>
<td>51</td>
<td>Richmond, VA**</td>
<td>1,627</td>
<td>26</td>
<td>Lower demand than average</td>
</tr>
</tbody>
</table>


Data above represents job postings from the past 12 months (March 2019-February 2019).

*All regions listed are Metropolitan Statistical Areas unless otherwise noted.

**These three MSAs comprise the Capital Region, for which there were 120,525 job postings requiring a security clearance in 2018.
FIGURE 4: EMPLOYERS IN THE CAPITAL REGION WITH THE MOST JOB OPENINGS REQUIRING A SECURITY CLEARANCE, 2018

HOW TO OBTAIN A SECURITY CLEARANCE

The key steps to obtaining and maintaining a security clearance are pre-investigation, investigation, adjudication, and reinvestigation.

An individual cannot simply apply for a clearance. There must exist a need by a Department of Defense organization for a job or service behind the clearance wall in order for a clearance to be offered. Direct hires, contractors, and military personnel are eligible for clearances. The Department of Defense Consolidated Adjudications Facility at Fort Meade issues security clearances for most Department of Defense civilians, military personnel, and contractor personnel. Other Department of Defense agencies that issue clearances are Defense Intelligence Agency, National Geospatial-Intelligence Agency, and National Security Agency. Executive Branch departments that issue clearances include the departments of Energy, State, Homeland Security, Transportation, Agriculture, Labor, Commerce, Treasury, Justice, Interior, Housing and Urban Development, Veterans Affairs, Health and Human Services, and Veterans Affairs. Many component agencies of these departments, as well as independent agencies (e.g. Central Intelligence Agency, Office of Personnel Management, Environmental Protection Agency, Government Accountability Office, Federal Communications Commission, International Trade Commission, etc.) issue clearances.9

The key steps to obtaining and maintaining a security clearance—outlined in Figure 5—are pre-investigation, investigation, adjudication, and reinvestigation. In the pre-investigation phase, the agency determines that an employee or contractor needs access to classified information in order to carry out his or her job. At the request of the sponsoring agency, the individual must then fill out clearance application materials.10 This includes Standard Form 86, which requires personal identifying data, as well as information regarding citizenship, residence, education, employment history, family and associates, and foreign connections/travel.11 Additionally, the form asks for information about mental health, criminal activity, drug/alcohol use, credit, and allegiance to the United States.12 The form is extensive and if an individual makes any mistakes or omissions on the form, it could delay the security clearance process.
The security background investigation begins after a person has been given a conditional offer of employment and has completed the security questionnaire (usually Standard Form 86). Investigators then verify the information an individual has supplied in his or her security package, including where he or she has lived, gone to school, and worked. Investigators may also talk to current and former neighbors, supervisors, co-workers, classmates, and the references the individual provided. Investigators contact law enforcement agencies in each of the places an individual has lived, worked, or attended school as well. A critical step in the background investigation is the face-to-face interview the individual has with an investigator. 13

In the adjudication phase, the results of the investigation are sent to the requesting agency’s security office. The adjudication phase is also the phase where a clearance candidate can “adjudicate” any discrepancies or special circumstances related to his or her investigation. This process is an important phase for the benefit of the candidate. The agency determines the individual’s eligibility for a security clearance and then decides whether to grant the clearance. 14

Security clearances are subject to periodic reinvestigation every 5 years for Top Secret clearance, 10 years for a secret clearance, or 15 years for a confidential clearance. 15 This requires the submission of an updated security package from the individual and another background investigation. The investigation will again cover key aspects of the individual’s life but will start from the previous background investigation. 16
REFORMING THE SECURITY CLEARANCE PROCESS

In June 2018, the White House announced an overhaul of the security clearance background investigation process, changing ownership of the process from the Office of Personal Management back to the Department of Defense.

The time it takes to process a security clearance has increased over the years. Recent processing times as of Q2 2019 range from 422 days for a Top Secret clearance to 234 days for a Secret Clearance. There is a backlog for a couple of reasons: (1) there is higher demand for cleared workers and consequently more workers need clearances, and (2) there is more for background investigators to investigate because there are more second-generation Americans with family members abroad, more communication activity due to social media, and more global connectivity in general, which leads to longer investigations, as investigators track foreign contacts and any potential illegal online activity.

In 2018, the security clearance process was put back on the Government Accountability Office’s High Risk list when investigations peaked at 725,000. In June 2018, the White House announced an overhaul of the security clearance background investigation process, changing ownership of the process from the Office of Personal Management back to the Department of Defense.

In June 2018, the U.S. Senate Select Committee on Intelligence introduced The Matthew Young Pollard Intelligence Authorization Act (IAA), which had the goals of breaking up the case backlog and hiring sufficient personnel—particularly in the STEM fields—to enhance readiness and protocols against cyber attacks. Though the bill failed, it is useful to examine as it laid out clear reform targets.
These measures aim to lead to:

1. Reducing the background investigation backlog to 200,000 by the end of 2019

2. Consolidating the background investigation function between the National Background Investigation Bureau (NBIB) and the DoD

3. Requiring Director of National Intelligence (DNI) to:
   - Reexamine the SF-86 questionnaire and the adjudicative standards,
   - Expand innovative techniques for investigative interviews (like Skype interviews),
   - Employ continuous evaluation instead of periodic reinvestigations,
   - Maintain consistent policies on interim clearances and treatment between government and contract employees, and
   - Make use of automated records checks from previous employers

90 percent of Secret and Top Secret clearances being processed within 30 days

90 percent of determinations regarding reciprocity made within 2 weeks

90 percent of clearance holders not needing reinvestigations on a preset periodicity (e.g., 5-years)
In 2019, the federal government introduced a new framework to consolidate and improve the security clearance process, which will be the biggest overhaul in 50 years. The Suitability and Security Clearance Performance Accountability Council has been working on the Trusted Workforce 2.0 Framework, which is the start of this security clearance process overhaul. Leading the council are representatives from the intelligence community, Department of Defense, Office of Personnel Management, and Office of Management and Budget. The result of this work is six central pillars, which is designed to streamline the adjudication process:

1. **More nimble policy making** – the framework creates a high-level guidepost for clearance work. A set of policy documents with more curated guidance for individual agencies and organizations to be released at a later date.

2. **Vetting tailored to mission needs** – the framework outlines five “vetting scenarios” to tailor the process to the need. The scenarios include: (1) Initial vetting for people who have not gone through the process before; (2) Continuous vetting that will replace the five- and 10-year periodic reviews with ongoing, and often automated, determinations of a person’s security risk; (3) Upgrading a clearance to a higher risk level; (4) Re-establishing a clearance after a lapse in continuous vetting; (5) Transferring clearances from one government agency to another.

3. **Aligned security, suitability, and credentialing** – this effort is currently split between OPM—which investigates whether someone is suitable for public service and issues proper credentials—and Office of the Director of National Intelligence—responsible for adjudicating whether someone is a national security risk. The framework looks to streamline the process.

4. **Reduced number of investigative tiers** – Once implemented, there will be three clear tiers of security clearances—public trust, secret, and top secret.

5. **Expanded spectrum of investigative methods** – in-person interviews will no longer be mandatory for every case. Digital and other secure interview channels can be used for lower-risk issues.

6. **Trusted information provider program** – The framework calls for establishing a program by which agencies and private sector organizations that conduct their own background investigation work can share what they’ve collected. This would be restricted to information and data—such as running a credit report—and not actual security determinations, officials said.
In 2019, the council will develop implementation policies for the 24 federal agencies that handle investigations as well as agencies and private sector organizations that employ cleared workers\textsuperscript{25}. In January 2019, Senator Mark Warner of Virginia re-introduced the bill\textsuperscript{26}, Modernizing the Trusted Workforce for the 21st Century Act of 2019, which, like the IAA bill, seeks to reform the security clearance process.\textsuperscript{27} In a press release\textsuperscript{28} on the bill, Warner said that the Modernizing the Trusted Workforce for the 21st Century Act would:

- Hold the Executive Branch accountable for addressing the immediate crisis of the background investigation backlog and provide a plan for consolidating the National Background Investigation Bureau at the Department of Defense, as the Administration has committed to doing;

- Implement practical reforms so that we can design policies and timelines for clearances that reflect modern circumstances. Reforms must be implemented equally for all departments, and for personnel requiring a clearance, whether they are employed by the government or industry;

- Strengthen oversight of the personnel vetting apparatus by codifying the Director of National Intelligence’s responsibilities as the Security Executive Agent; and

- Promote innovation, including by analyzing how a determination of trust clearance can be tied to a person, not to an agency’s sponsorship. The bill draws on provisions that were contained in the Intelligence Authorization Act unanimously reported out of the Senate Select Committee on Intelligence in June 2018.
Employers in the region are greatly affected by the high demand for security clearances. One of these employers is Apex Systems, a Richmond-based IT staffing and workforce solutions firm that specializes in providing IT professionals for contract, contract-to-hire, and direct placements. The backlog affects Apex Systems’ Capital Region placements. Moe Elnabawi, National Practice Director of Government Services at Apex Systems said: “In our D.C. Federal Branch alone, we have upwards of 120 plus offers pending a clearance process at any given time—these are people who have accepted an offer and are waiting to go in [to work]. If you look at similar sized Apex branches, they usually only have about 20-30 placements pending at any given time—these are people who have accepted an offer and are waiting to go in [to work]. If I had to put a number on it, I would say we probably lose about 20-30 percent of placements by the time they are cleared.” Clay McNerney, Practice Director for Intelligence Sector Delivery at Apex Systems, also emphasized the effect of security clearance backlogs on his work: “Right now, I have over a dozen people in some level of clearance processing whose offers were extending between December 2018 and February 2019 who still have not started...it's averaging 44 days for individuals to start. That is compared to about 10-14 days for the commercial market.” There is a clear economic benefit to reform this process and clear more workers, leaving fewer jobs unfilled.

Another issue that arises due to such a controlled supply of cleared workers is that employers often must fight for cleared workers and end up poaching cleared employees from each other. As a result, some employers will lose staff in which they have invested substantial resources to recruit and train. Penny Cantwell, Vice President at Sandy Spring Bank and Board Member at the Fort Meade Alliance voiced this concern: “Nobody wants to be the one who brings people in, trains them, and then loses them to another employer.”
them to another employer." There is also a premium on employees with security clearances. Clay McNerney of Apex Systems gave an example: "If a mid-level Java Developer with 5 years of experience and a bachelor’s degree in computer science makes $100,000 in the open marketplace, with a Top Secret Security clearance, that Java Developer would be worth 15-20 percent more. If the position requires a full polygraph clearance, that salary increase has at least a 25 percent premium." Reforming the process and increasing the digital tech talent pipeline would mitigate this issue.

Another pressing problem is rapid technological changes. Tim O’Ferrall, General Manager of the Fort Meade Alliance, explained that "technology changes so quickly that the missions require both speed of innovation and acquisition to keep up with global threats and competition." O’Ferrall said: "We need candidates to move through the clearance process properly and quickly to meet the demand."
Various groups within the Capital Region are already working to address the challenges that impede more proactive talent planning and project delivery for initiatives requiring cleared workers. This section outlines considerations for how the federal government, employers, and higher education institutions can continue taking steps to improve the security clearance process.

**FEDERAL GOVERNMENT**

Federal reform is central to improvement of the security clearance process. Recommendations for the federal government include:

1. **Act quickly and effectively to address the security clearance backlog in 2019**, so the Capital Region can fill security clearance jobs and move towards reaching its full economic potential. The federal government is already rolling out the Trusted Workforce 2.0 Framework with the goal of improving the process. The council creating the framework will develop implementation policies for the 24 federal agencies that handle investigations as well as agencies and private sector organizations that employ cleared workers in 2019, but meaningful changes cannot go into effect until the policy work is complete. The failed IAA bill called for a reduction of the investigation backlog to 200,000 by the end of 2019—the backlog has now been reduced to approximately 550,000,\(^{21}\) which is still far off from this call. The Modernizing the Trusted Workforce for the 21st Century Act of 2019 recently introduced in the Senate also seeks to address the security clearance issue.

2. **Clarify how contracts are written to help recipients more effectively plan around the security clearance process.** This may include extending project timelines, extending interim clearances, and clearly allotting a percentage of employees that can work on a contract without a security clearance. This will help employers be more proactive about staffing plans and worker retention.
1. **Tap into military transition assistance programs to find more new hires with security clearances.** Some companies have had success training these candidates so that when a contract opportunity arrives that requires cleared workers, the companies have the manpower to execute the contract.

2. **Extend interim clearances to enable employees to complete contract work.** If a worker passes an initial National Agency Check with Inquiries (NACI), he or she can work on certain contracts with an interim clearance. This clearance can be extended on a case-by-case basis, depending on the role and level of access on the contract. Employers can also get creative about staffing in a way that allows employees to begin working on internal systems before being deployed.

EMPLOYERS

While policy reform is critical to addressing the backlog of security clearances, employers can consider various strategies to alleviate the strain on the talent pipeline in the short- to mid-term. Strategies for employers include:
Help increase the pipeline of students that are prepared for roles in digital tech. Education providers in D.C., Maryland, and Virginia—which train students who then enter the Capital Region’s workforce—increased the number of awards from digital tech-related programs by 52 percent between 2010 and 2017. Yet, in 2017, there were only 20,270 digital tech awards granted for 209,957 digital tech job postings in the region.33

One group that is tackling this challenge is the Greater Washington Partnership’s Capital Collaborative of Leaders in Academia and Business (“CoLAB”), which is an action-oriented partnership that brings together the leaders of the region’s top academic institutions and businesses to make the region a leading global hub for innovation. CoLAB businesses and universities have been working collaboratively to develop digital technology credentials to increase the quantity and quality of digital technology talent emerging from local undergraduate programs.

Prepare and encourage students to pursue internships that may start the security clearance early. Federal agencies and defense contractors roll out internship opportunities every year, and some of these opportunities involve security clearances.

For example, the partnership between the National Security Agency (“NSA”) and University of Maryland, Baltimore County (UMBC), exposes students to subjects critical to national security and helps them prepare to enter the national security workforce. UMBC is a National Center of Academic Excellence (CAE) that promotes higher education and research in the critical area of cyber defense. CAE schools produce professionals with the expertise to reduce vulnerability in the national information infrastructure. The NSA and UMBC partner on research, and the NSA sponsors a scholars program (UMBC Meyerhoff Scholars) to give students a chance to interact with NSA employees and learn about careers at the NSA.34 This partnership strengthens the talent pipeline and encourages students to apply for internships and jobs in the national security field, which allows for some to start the security clearance process early.

Many federal agencies conduct clearance prep workshops that teach university students about security clearances and the clearance process in general. This is a great opportunity for students to ask clearance officers questions about the process and learn more about careers in national security.
1. Federal spending information is from USAspending.gov. Federal job information is from the Bureau of Labor Statistics (data as of Q42018). This does not account for federal contracting jobs.
2. We define “digital tech” workers as a group of workers comprising 20 technology-oriented occupations. The full list of workers can be found in the Greater Washington Partnership’s report, Partnering to Strengthen Tech Talent in the Capital Region.
7. Ibid.
24. Ibid.
25. Ibid.
26. Warner first introduced the bill to the 115th Congress in December 2018. It was read twice and referred to the Select Committee on Intelligence.
About Apex Systems: Apex Systems combines with parent company ASGN Incorporated to be the 2nd largest IT staffing and services firm and 3rd largest clinical/scientific staffing firm in the U.S. Founded in 1995 and headquartered in Glen Allen, Virginia, Apex utilizes specialized technology and industry practice groups to deliver the most talented and qualified technical professionals to clients within all major industries. Apex has a presence in over 70 markets across North America with contractors currently placed in companies throughout the U.S. and Canada. In 2018, Apex had over 44,500 contract employees on assignment. To learn more visit www.apexsystems.com. (NYSE: ASGN)

The Fort Meade Alliance launched an initiative called Project Scope that aims to educate students in middle school, high school, and college about security clearances. For more information, please visit http://project-scope.org/.


Interview with experts, April 2019.


The Greater Washington Partnership is a first-of-its-kind civic alliance of CEOs in the region, drawing from the leading employers and entrepreneurs committed to making the Capital Region—from Baltimore to Richmond—one of the world’s best places to live, work and build a business.