IT Alliance for Public Sector
A Division of ITI

Testimony of

A.R. "Trey" Hodgkins, III

Senior Vice President
IT Alliance for Public Sector

before a hearing of the

Subcommittee on Government Operations

of the

U.S. House of Representatives
Committee on Oversight and Government Reform

Wednesday, October 11, 2017

Introduction

Chairman Meadows and Ranking Member Connolly, thank you for the opportunity to share industry perspectives on the challenges industry and the federal government face in regard to the broken security clearance process. We applaud and encourage your oversight of the process and would hope that your attention will drive reform and modernization to the very serious threat the current state of the security clearance process poses.

The 21st century has brought new and ever evolving threats to our national and homeland security from inside and outside of our government and beyond the borders of our nation. Government agencies and departments have increased their reliance on private sector partners to contribute to the diverse national and homeland security missions. Unfortunately, the security clearance process has not adapted or sufficiently modernized to meet these demands and enable the government and industry workforce it takes to meet these new mission imperatives.

While the backlog of clearance applications is a major cause for convening this hearing, we hope that Congressional attention does not get lost on this recurring short-term symptom of a larger systemic problem. We recognize that as your partners in the federal contractor community, we do not hold a monopoly on the pain inflicted by the current system. The backlog impacts the ability of the federal government to investigate applicants and determine their suitability for employment, just as much as it impacts the ability for contractor personnel to get a clearance to work on a contract. We believe that holistic, government-wide security clearance reform should be the objective, as it is imperative to both security and productivity. As we move to reform the process, industry remains agnostic as to who "owns" the security clearance process; we are, however, resolute that any bifurcation to the process would only cause greater wait times, inefficiencies, waste taxpayer dollars, potentially create greater vulnerabilities, and undermine achieving a truly reformed clearance process.

A Brief History Lesson

The current predicament is not new. There are decades of reports from the Government Accountability Office detailing the challenges with the security clearance process and the backlog of applications. We must also recall that the security clearance process has been bifurcated in the past, with the Department of Defense (DOD) owning the investigative portion for DOD applicants as recently as the latter part of the last century. In fact, it was the inability of the Department to effectively manage the volume of investigations in that era that led to the consolidation of most of the government clearance and personnel investigative functions at the Office of Personnel Management (OPM). It was also the inability of OPM to effectively absorb that existing DOD backlog into a consolidated process that created the backlog problems of the early 2000s. We have seen these challenges before and recommend that Congress act now to not only address the short-term symptoms of the latest backlog of applicants, but also to invest in a permanent effort to address the systemic challenges of the security clearance process.

Executive Summary

The current the backlog of clearances awaiting investigation sits at over 700,000, a number that is unacceptable by any metric. Unfortunately, the immediate crisis that backlog creates is only part of the problem, as it injects increased risk into an outdated system that does not leverage the digital era to create a more effective security environment and which continues to inefficiently spend taxpayer dollars.

In the early 2000s, I worked with a coalition of industry trade associations who partnered with government stakeholders to identify the problems with the security clearance process that time, implement a long-term solution to resolve the situation, and create a pathway of process reform, modernization, and improvement. The situation improved in the wake of aggressive Congressional oversight by this Committee and others, culminating in the security clearance process reforms of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Unfortunately, the departure from that pathway of reform and modernization has contributed to the current state of security clearance processing.

Because we have gone back to the future with our current state, resulting in exorbitant wait times, ballooning costs, and systemic inefficiencies, ITAPS has re-convened the broad and diverse industry coalition to help assess the problems, and to suggest short and long-term solutions. In conjunction with our partners at the Aerospace Industries Association, the Association of General Contractors, the National Defense Industrial Association, the Professional Services Council, and the U.S. Chamber of Commerce, we have met and spoken with government stakeholders over the course of the past year. These stakeholders include the House and Senate Armed Services Committees (HASC/SASC), the House Permanent Select Committee on Intelligence (HPSCI), the Senate Homeland Security and Governmental Affairs Committee (HSGAC), the House Oversight and Government Reform Committee (HOGR), the National Background Investigation Bureau (NBIB), the Defense Security Services (DSS), the Office of Undersecretary of Defense for Intelligence (USD(I)), the Performance Accountability Council Project Management Office (PAC/PMO), and the Information Security Oversight Office (ISOO) at the National Archives.

At the time of the reforms of the IRTPA, industry brought forward a set of criteria to help guide the development of proposals and solutions to resolve the challenges the security clearance process faced. After our extensive engagement with stakeholders to assess the challenges we face today, we would submit to this Committee and others that those suggestions and criteria are still applicable and deserve resurrection to guide efforts to reform, modernize and improve the security clearance granting process today. We identify these suggestions as "The Four Ones":

- One application
- One investigation
- One adjudication
- One clearance

We have also advanced technologically and there are several options that can be applied to the process to improve efficiency, establish real-time monitoring of clearance holders, and better enable the counterintelligence mission to take stock of those trusted by the government. My recommendations and testimony will outline what each of these means, why we believe these criteria for reform still hold merit in today's situation and discuss the technological capabilities that can be applied at each step to enhance and improve the process.

Sadly, because these criteria still have merit today, it is a clear indicator of just how little has actually been improved in the clearance granting and maintenance processes. Adopting the Four Ones and the technological options will lead to a common operating picture, which we believe is the necessary end state for resolving the current challenges and positioning the process where it is ready for the threats and challenges of the new century.

Following the hack of OPM, on October 1, 2016, the NBIB was created to absorb OPM's Federal Investigative Services (FIS) and enable a centralized security clearance process. The FY 2017 National Defense Authorization Act (NDAA) required a report[1] from the Secretary of Defense (SECDEF), that was due on August 1st, 2017, detailing how the Department of Defense would move the investigation of DOD clearance applicants to the Defense Security Service (DSS), and on October 1, 2017, a plan was due from SECDEF and OPM on how to transfer these authorities. With barely more than a year passed since the creation of NBIB, a plan has already been developed to bifurcate the clearance process. Industry is concerned that such a bifurcation will undoubtedly lead to further and compounding inefficiencies. Additionally, this plan moved forward so quickly that DSS published an RFI on FedBizOpps.gov[2] on September 20, 2017, requesting: "market research to gather data for the purpose of developing requirements to contract for investigative service providers to conduct background investigations on Department of Defense (DOD)-affiliated personnel." The conflation of the reporting timelines, along with the issuance of the RFI, show that this process is anything but collaborative and measured and is not taking into account the detrimental effects it will create on the clearance granting process government-wide.

The Senate Armed Services Committee (SASC) included a provision, Section 938, in their FY 2018 National Defense Authorization Act (NDAA), S. 1519, that would move DOD clearances and the process surrounding them, back to the Department. The SASC recognized that something must be done to resolve this latest bout of problems with the security clearance system. We must oppose Section 938, however, because it does not adhere to the criteria of the Four Ones and will create a parallel process and duplicative regime in the Department that will increase costs and drain resources, cause further delays, hinder process improvements, and undermine efforts to move the government toward true reciprocity across all departments and agencies.

Despite prescriptive actions by Congress to address this systemic and enduring issue, problems persist. It will take Congressional oversight, Executive enforcement, and agency/department leadership to see meaningful changes implemented in the security clearance process. Finally, we hope to work with you to address the security clearance problem in a holistic, government-wide fashion. If the government seeks to deliver a more efficient, thorough, and secure process, it must include end-to-end digitization, shared services, utilize continuous evaluation, and leverage private sector partners for success.

Background

In order to perform many critical services for government customers, hundreds of thousands of industry personnel must obtain and renew security clearances every year. The security clearance process, rules, and regulations are very important to industry because they create the mechanism to obtain and clear qualified personnel to support the government's critical missions. Our suggestions, however, are not solely designed with industry goals in mind. Instead, our recommendations take a "whole of government" approach designed to create a system and processes that enable greater national security. Indeed, government employees, the priority in the security clearance process, are sure to benefit. We humbly recognize that national security is an inherently governmental function. Yet, it is the industrial base that provides critical capabilities to the government that enables mission success.

[1] Section 951, FY 2017 NDAA
[2] https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=38f74a6d1e492540bf7aed8d470efdd8

Industry faces increased pressure to deliver cleared personnel on the day a contract begins. The current state of the clearance granting process makes it almost impossible for industry to meet these demands. These delays in obtaining security clearances result in increased costs to the federal government, and ultimately the taxpayer, by delaying the ability to use the most qualified personnel on critical programs. In fact, industry has turned to "poaching" already cleared personnel to deliver contract needs. This process unnecessarily inflates costs of contracts and is the reality of a broken system. These costs run into the hundreds of millions of dollars for both government and industry. It also stifles innovation and cooperation, since it is virtually impossible to share a good idea or leverage an existing team to provide solutions across agencies or departments without having appropriately cleared personnel. Ultimately, we can only conclude that a considerable amount of important work is not getting done.

In the wake of the OPM breach of cleared personnel data, there was a contract to provide credit monitoring and restoration services for each person known to have had their records stolen. To pay for this contract, OPM apportioned the costs across their customer base. Many agencies, like DOD, lacked sufficient funding to both pay for new investigations and cover their portion of the contract, so the funds were used to pay for the service. Only when additional funding was identified were the agencies able to restore submission of applications for investigation. However, the ability to find an adequate number of qualified investigators to meet the investigation demand signal still perplexes the government. Bifurcating that process would only make that problem worse, while increasing costs.

One Application

"One application" envisions that an applicant would complete one standardized and digitized application that would become the permanent digital record and security history for an applicant and, if deemed suitable, a clearance holder. The "one application" goal made progress with the implementation of the e-QIP application format. NBIB is also rolling out in the near-term an updated, digitized Standard Form 86 (SF86). Standardization across the application process, however, is still lacking.

Also submitted with the digital application are fingerprints and signatures, which form the completed application package. Any one of these elements, if not submitted concurrently, can expire and delay initiation of an investigation, so coordination on submission is critical. In the effort to technologically enable the application process, the efforts to digitize fingerprinting is an area to be commended as, per NBIB, 94% of fingerprint collection is now done electronically. The next step in the process needs to be a digital signature and digital transmission, to a centralized database.

From this continuously accessible, digitized central repository comes the beginning of the total security history of an individual. As other elements of the Four Ones noted below, like continuous evaluation, become the norm in the national security process, we must enable the evaluation component from the beginning. Today, investigators are only given a static snapshot with which to judge a dynamic environment and dynamic individual. In the current process, such examinations only happen during the initial application and investigation, and thereafter only at 5-or 10-year intervals depending on the level of the clearance. We must also examine other elements that form the individual record, like foreign contact disclosure reports and other addendums, which are still handwritten, and move toward complete digitization of the forms and electronic submissions to the same repository to be appended to the total security history. Moving toward "One Application" would therefore enable dynamic access to the security history of a cleared person. Technology can enable all of these capabilities now.

One Investigation

One Investigation is vital to the continuity of the security clearance process and critical to the ability to achieve One Clearance, discussed later in my testimony. Unfortunately, agencies have historically disregarded investigations conducted on an individual and initiated a new process, even though the individual has already been investigated and has been granted a clearance. While this practice was statutorily prohibited in the IRTPA, it has not stopped agencies from refusing to accept the investigative conclusions of other agencies and many take the liberty to execute additional scrutiny of an individual. Many in government and industry are very familiar with the situation where personnel carry a multitude of different badges, each representing another examination.

Congress should examine this practice and determine if additional legislative prohibitions are necessary. At the very least, these re-examinations cause further delay in the overall effort to get cleared personnel on contract or in a mission area, and they can be a redundant, wasteful use of taxpayer funding. Congress should require uniform, government-wide standardization of the investigative process, protocols, and vocabulary employed to achieve One Investigation. Such an outcome would produce an investigative record that can be reviewed and interpreted consistently across government.

Technology also allows us to move beyond the static investigations of today because security situations are dynamic, and so, too, should be the investigations. In order to create a dynamic security situation, we should move toward continuous real-time evaluation of all clearance holders. One investigation becomes not only the initial investigation of an individual, but also a continuous analysis of public and private data sets for indicators and anomalies related to clearance holders. Continuous evaluation would also obviate the need for periodic reinvestigations at the 5-year (Top Secret) and 10-year (Secret) intervals.

Periodic reinvestigations (PR) are another key component in the clearance granting process badly in need of attention. In order to slow down the volume of investigations and avoid increasing the backlog at NBIB, agencies have taken extraordinary measures to extend clearance viability beyond the time requirements for PRs. Reinvestigations have been relegated to such a low priority that clearances held by industry personnel working on government projects sometimes expire before any action is taken to complete the renewal application. The condition is such that many periodic reinvestigations are considered to be "in process" once the clearance holder has completed an application for reinvestigation. In reality, many such applications are never entered into the process because the emphasis is placed upon those who do not have clearances, under the assumption that those with a clearance can be placed in a lower priority and be processed at a later date.

For government, this may seem to be an acceptable temporary solution. In practice, industry finds that more and more frequently, clearances have lapsed. These discoveries are made when cleared personnel try to move from contract to contract, start supporting a new agency under an existing contract, or relocate or get new employment and the validity of their clearance must be checked. It is at this time that both the employer and the clearance holder frequently first discover that, despite the completion of the periodic reinvestigation application, the paperwork was never processed and the clearance is "out of scope." Therefore, current clearance holders are now at even greater risk of having their clearance expire and/or lose their SCI access.

If we migrated to a One Investigation dynamic that included continuous evaluation, we can watch for the appearance of any "flags" or indicators (e.g. multiple foreign trips, foreign disclosures, divorce, financial

trouble, sudden financial gain, social media activity) that would show the need to reinvestigate an individual. In a situation where a cleared individual receives a clearance, and the very next day all these flags populate in an automated system, it would be pertinent and proper to investigate these occurrences rather than waiting 5 (TS) or 10 (S) years to delve into these issues. The consumer analogy is the real-time monitoring of credit by financial institutions. Charges to credit cards that appear fraudulent are immediately alerted to the consumer. This "real-time" condition should become the expected standard of investigation and evaluation of anyone with a clearance. But, reinvestigations are prescriptive on an arbitrarily determined timeline. In order to assess the status of this condition, industry would recommend that a survey of the backlog be conducted to determine exactly how many of the overdue applications are still valid, what steps be taken to ensure that cleared personnel are effectively scrutinized as appropriate, and that the clearances of industry personnel are not placed in jeopardy of being "out-of-scope."

One Adjudication

Industry has long sought standardization and uniformity in the process of adjudication and suitability determinations so that a person holding a secret or top-secret clearance could be confident that there would not be variances in the interpretation of their adjudication from one agency to the next. A uniform, government-wide adjudication standard will allow private-sector partners to rapidly execute on contracts. We recognize that suitability determinations may be different for the various level of sensitive work conducted within the government. A modular, building block type of suitability system, however, that even the least sensitive positions are investigated the same as the most sensitive, will produce common data and process. This will not only enable uniform insider threat data, but it will allow government and private sector employees to move from one department or agency to another with relative ease.

As one contract with an agency or department concludes, the need to move personnel to other contracts exists industry-wide. There is no salient argument for different adjudication standards across various government agencies and departments. The condition, however, is not limited to just the private sector. Federated U.S. government entities, such as DOJ and DHS, with multiple component agencies frequently do not acknowledge clearances issued within the same department. The concept of "one adjudication" builds upon the uniformity and standardization discussed above and leads directly into the following stage – one clearance.

To be commended, at this point in time, adjudication is the least problematic step in the process for industry. Once the investigation stage has been completed, the investigation record is returned to the requesting agency that is responsible for making the determination about suitability and eligibility and issuing the clearance. The most rapid portion of the security clearance has been, and continues to be, adjudication. Yet, even adjudication can be improved upon by standardizing the process.

One Clearance

Cleared professionals access much of the same systems, Secret Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communications System (JWICS), across government, so that all-source intelligence can help inform a common operating picture. Clearances, however, are not treated in the same manner.

One reason for the persistence of the conditions outlined in this paper is the lack of a single, government-wide, interoperable, real-time database containing all clearance and access information. The database

containing this information for the intelligence community, Scattered Castles, is classified and not linked to the same unclassified but sensitive database for the civilian and defense agencies- the Joint Personnel Adjudication Systems (JPAS) - which is slated to be replaced by Defense Information System for Security (DISS). There are also defense and civilian agencies that do not contribute information to the databases in a timely manner, making the clearance information issued by them incomplete or unreliable. Another hurdle to overcome is the requirement by some agencies to only recognize up-to-date clearances, (i.e., based upon a current investigation), even though the delays discussed above are pushing "active" clearances beyond their standard periodic reinvestigation timeframes. These requirements must be corrected for reciprocity to work as Congress envisioned it.

We have seen some improvement in the reciprocity of clearances, particularly in the intelligence community[3] with 86 percent reciprocity government-wide but instances when agencies refuse to recognize each other's clearances still occur with regularity. Another improvement industry has noted is the reduction in cases requiring a re-investigation of a current clearance by a second or third agency. Other onerous requirements short of a re-investigation, however, are still sometimes imposed and they serve only to slow down the process, duplicate efforts, increase the burden on taxpayers for redundant government activity, and prevent the agency from meeting its demands in a timelier fashion.

Ultimately, Congress and the Administration must require Federal agencies to provide accurate, timely, and thorough information about the clearances each has granted. This will enable the capability for others, when authorized, to review applications, the subsequent investigations, the results, and finally, the basis for adjudicating a clearance positively so that reciprocity can be fully realized wherever the national security needs of the United States demand.

Each agency has its own rules that prohibit smooth, timely movement of cleared contractor personnel from one contract to another. Despite prescriptive statues and guidance directing reciprocity, there is not reciprocity in practice.

The cost of doing business:

A systemic issue our coalition discovered was the cost of a security clearance is dynamic, versus fixed, throughout a fiscal year. DSS is reliably able to predict in a given year roughly how many investigations will occur. In doing so, expectations are established about the width of the investigation pipeline, which informs customers. However, between this prediction and execution, the cost of a clearance can and does change. This disparity leads to unfulfilled investigations due to budgeted versus actual investigations able to be executed in a fiscal year. Director Phalen of the NBIB has executed a fix to this issue, however, it is not in statute. We commend his leadership on this. We recommend that this change be codified so that future costs are known and able to be planned for, creating a measure of predictability and reliability in the security clearance process.

Conclusion:

Though this hearing was held to address security clearances in the present tense, we would be remiss not to point out future technology trends that will enable greater information and personnel security. Utilizing emerging technologies, like blockchain, to secure information and enable the trusted information

[3] https://federalnewsradio.com/workforce/2017/02/security-clearance-reciprocity-86-percent-governmentwide/

exchange among multiple parties through a shared ledger must be part of the conversation. Utilizing artificial intelligence to monitor trusted user activity, building usage profiles, and sharing it among all other agencies, will also create a roadmap to reducing risk. Finally, applying big data analytics to the data on all past and current clearance holders can help identify and develop better counterintelligence means to address threats. Siloed department and agency efforts to eliminate the insider threat problem only harms the greater good. This problem is not unique to any agency or department and the government must tackle the issue holistically.

Systemic issues still exist, enabled by arcane, bureaucratic red-tape, that promote distrust, slow favorable outcomes, and increase cost to the American taxpayer. Despite repeated prescriptive measures by multiple Congressional committees, the security clearance issues persist. From backlogs of 600,000 in 1999[4], to a low point in the first decade of the 21st century, and now 700,000, the cycle must stop by enacting true reforms.

In a "whole of government" approach, a singular authority must own the entire security clearance process – for security and accountability's sake. In this no-fail mission, a singular entity should standardize all processes and reign in the disparate systems and procedures that exist today. As security clearances are no more than a combination of a continuous counterintelligence investigation and operational security, it is incumbent to standardize and centralize the process with "The Four Ones".

It cannot be overstated that industry is committed to preserving the strict government requirements to obtain security clearances. The process, however, must be optimized to include leveraging industry relationships and deploying technology across the process. The interest is not to minimize current requirements, but to make appropriate changes to an antiquated process. This would allow the nation to remain vigilant in determining who has access to sensitive information while better meeting defense and intelligence needs at the lowest possible cost. Industry looks forward to working with the government to examine and implement these and other recommendations, and stands ready to devote its experience and significant expertise with best practices to ensure that critical government programs do not go unexecuted for lack of available cleared personnel.

Thank you for the opportunity to share our perspectives with the Committee.

RECOMMENDATIONS FOR CONGRESS AND THE ADMINISTRATION

1. Reinvigorate previous efforts to create one electronic record across a continuous digital process for clearances.
2. Tap the expertise of leading technology companies to partner with the national security community to apply new technological solutions to rethink the entire clearance process.
    a. DIUx, DARPA, IARPA, and In-Q-Tel enable wonderful outcomes, it's time to unleash them and others, on this problem.
3. Ensure that the security clearance process – from application, to investigation, to adjudication, to re-investigation – is technologically enabled; do away with paper files and ensure that all systems are interoperable and can share data across platforms and agencies.
4. Codify NBIB authority to align fee-setting with fiscal years, instead of allowing the practice to occur after budgets are fixed.

[4] http://www.gao.gov/products/GAO/T-NSIAD-00-148

5. Move from the mindset of a security clearance "process" to that of continuous evaluation.
    a. Just like counterintelligence and operational security is a dynamic process, so too should the security clearances process.
6. Enable information from employers to be used as a part of the security clearance investigation (e.g. college transcripts, previous employment history, etc.).
7. Establish a singular system of record, utilized by all 16 intelligence agencies and corresponding departments, that verifies the existence of a security clearance, without the clearance needing to be "passed."