

STATEMENT

OF

Doug Wagoner

**Chairman, ITAA Intelligence/
Security Clearances Task Group**

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

**CONCERNING THE
ISSUANCE OF SECURITY CLEARANCES BY THE
FEDERAL GOVERNMENT TO INDUSTRY CONTRACTOR
PERSONNEL**

ON BEHALF OF

**INFORMATION TECHNOLOGY
ASSOCIATION OF AMERICA**

May 6, 2004



Introduction

Mr. Chairman and Members of the Committee. Thank you for inviting the Information Technology Association of America (ITAA) to testify today on the issues affecting the government contracting community as a result of backlogs, lack of reciprocity, and severe delays in the granting of security clearances that are taking over a year to complete to get someone working on classified government support project. Industry seeks to work with the government to get that time down to 120 days over the next two years. As an association, we would favor a statutory performance metric that will require clearances to be completed in this time frame rather than provisions that would specify how to accomplish the time reductions.

My name is Doug Wagoner, and I serve as Vice President and General Manager of Data Systems Analysts, Inc. (DSA), a small IT services company in Fairfax, Virginia. I'm here today, however, in my role as Chair of ITAA's Intelligence Committee, which was established in November 2002 following consistent calls from the ITAA membership for assistance from their trade association in resolving the tremendous burdens and challenges IT contractors face with this vital component of national security.

As you know Mr. Chairman, ITAA is the nation's leading and oldest trade association focused on the diverse information technology (IT) industry, and provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of more than 400 corporate members throughout the United States, and serves as the Secretariat for the World Information Technology and Services Alliance (WITSA), a global network of 50 countries' national IT trade associations. ITAA represents virtually every major federal IT contractor and many other public and private sector contractors, and counts among its membership a wide range of companies from the largest enterprise solutions providers to the smallest IT start-ups. The Association takes the leading role in major public policy issues of concern to the IT industry, including government IT procurement, homeland security, information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy protection, and e-commerce, among others.

The federal government continues to rely heavily on commercial industry partners to fulfill critical government services. The sheer magnitude of commercial activities in support of the government necessitates that government and industry work together to ensure the best private sector personnel are available to fulfill critical government needs. In order to perform many of these critical services in partnership with government, industry personnel must obtain and renew security clearances. The current security clearance process, rules, and regulations are very important to industry and create a mechanism that we believe must be improved upon in order to better safeguard the national security by permitting industry to hire and clear qualified personnel in a timely fashion. As we deal with new asymmetrical threats in our ongoing war on terrorism, government's industry partners face increased pressure to deliver cleared personnel on the very day a contract begins. The current delays being experienced by contractors in obtaining security clearances prevents this from happening and as a result, delays performance on critical programs and increases costs to the federal government in the form of higher labor costs and protracted contracts.

It's important that we note as we begin this hearing Mr. Chairman that these challenges and concerns are not new. While the pressures placed on an already stretched system because of heightened security demands following the September 11th attacks certainly have exacerbated the problems in the system, the challenges we face have been the same for decades. In fact, since the early 1980s, if not earlier, the issue has been raised in the Congress, the Executive Branch, and oversight bodies such as the General Accounting Office in the hope that some changes can be made to what is a vastly complicated and highly repetitive process across government. The problem is certainly more pronounced now because of higher demand, but the core challenges remain the same. Industry (and government personnel in need of clearances) is still seeing a more than 12 month time period for the issuance of a new Top Secret DOD clearance – this is the average for a “clean case” where an individual has had limited foreign travel, and has no credit or police problems. Clearances requiring more extensive investigations, including a polygraph, are routinely taking 16 months or more to complete.

Within the ITAA membership, the current delays in obtaining security clearances consistently ranks #1 or #2 among the chief concerns our members have in their ability to effectively do business with the federal government. Since our members businesses are built around partnership with the government, the inability to deliver cleared personnel directly prevents them from meeting critical government missions and priorities. Given the role the IT community plays in enabling digital government and the information sharing that is so vital to government efficiency and homeland security, we believe our members' experience with the challenges in obtaining security clearances represents an accurate model of what other contracting sectors have experienced with this issue. In other ways, our members' experiences represent an even more acutely

important example given the role of information technology in government operations. Quite simply, if our members are unable to meet critical mission needs, the downstream mission areas dependent on information technology will also be hindered.

In addition to the personnel security clearance process delays, the failure of federal agencies and Departments to honor existing regulatory requirements, such as those mentioned in the body of this testimony, causes inordinate and unacceptable delays in moving personnel with existing clearances and special accesses from one contract or supported government customer to another. These actions can and should be accomplished in minutes, not months, simply by adhering to existing regulatory requirements and deploying technologies and management practices that are well developed.

Before I detail ITAA's recommendations to reduce the time to clear both government and industry personnel, I cannot emphasize enough that industry in no way wants to diminish our nation's security posture by reducing the important standards that govern who has access to sensitive government information. My committee worked for the better part of the last year to create these recommendations. The time involved was due in large part to constant review by security experts to ensure our recommendations would not negatively impact security. Industry is committed as a trusted partner of government to safeguarding national security information; we believe, however, that much can be done to improve the current process without diminishing this fundamental goal.

In November 2002, ITAA formed a task force to deal with the increasingly important issue of security clearances. I am honored to serve as the Chairman of this task force, which is comprised of senior executives from ITAA member companies whose collective experiences encompass the full range of industrial and personnel security disciplines. Several members of our task force have served in senior level security positions within the defense and intelligence communities, and most have gone through the clearance process multiple times as part of their government or military service, and now, as industry partners with the government on mission critical programs.

When our task force initially convened, we spent the first several meetings sharing "horror" stories about the process. Without exception, members of our task force were able to recount in remarkable detail untold numbers of bad experiences they have had with getting their personnel cleared to work on specific programs. As we explored the "horror" stories with our members, we also received startling statistics from our members that drove home just how significant a problem this is for industry; time and time again, we were told that particular companies have several hundred or even thousands of positions open that require clearances for which they cannot find suitable cleared candidates to fill in a timely manner.

We will discuss some more formal statistics in greater detail later in our testimony, but these anecdotal stories are reinforced every day here in Washington on our radio waves and in print and television advertising. Ultimately, what this issue comes down to is jobs: there are literally thousands of job opportunities available here and around the country that cannot be filled because there isn't a large enough population of cleared workers. And one of the major reasons there isn't a large enough population of cleared workers is because there also aren't sufficient investigators available to ensure the timely completion of new background investigations. If you've listened to National Public Radio (NPR) or WTOP while you've sat in Washington traffic, I have no doubt you've heard the countless ads played over and over again from local technology companies seeking applicants with current clearances. My company is among those that have turned to the airwaves to solicit cleared personnel.

A current clearance that can be put to work immediately for a company is worth 10 times its weight in gold. If you go to any job fair here in the Washington area and tell recruiters you have an active clearance, you can probably walk out of that event with multiple job offers. Job seekers with active clearances know this, and we're seeing startling trends where employees move from company to company every 6 months because they're lured away by higher salaries from competing companies. Each time the employee moves around, his or her salary may jump 10%-25%; while this is good news for the employee, it significantly increases costs to the company. These costs are most often passed back to the government in the form of higher labor rates for specific employees working on a contract. The associated turnover when employees jump from one company to another also disrupts critical government programs that become short-staffed upon the departure of key personnel.

ITAA has heard for several years a lot of anecdotal information from member companies about the challenges and pains they experience with the security clearance process, but we wanted to make sure we had real statistics to share with you today, so we developed a survey instrument to poll ITAA members with some very specific questions about their experiences with this critical process.

While it is unknown what the total current number of cleared contractor job vacancies is across government, it is clear the number of openings from company to company is staggering. ITAA asked its member companies to identify the number of current openings in their company that require security clearances. Nearly 50% of our survey respondents indicated having less than 50 current openings that require clearances, but a staggering 22% of respondents indicated they have 500 or more positions open that require some level of clearance.

Nearly 70% of respondents indicate that the clearance process is restricting their ability to grow their company; small companies in particular have a difficult time

filling significant numbers of positions in a short time period. Take my company DSA as an example; at the end of last fiscal year, we were fortunate enough to win several contracts we bid for work at DoD and within the Intelligence Community. Our company currently has only about 150 employees. These new contractual obligations required that we hire approximately another 50 individuals. We have purchased advertising on WTOP and tried every other recruiting tactic we know, but as of this hearing, we still have 40 positions open.

On the topic of recruiting methods, the ITAA survey also asked member companies to document how they primarily recruit new talent for work requiring security clearances. Fifty-four percent (54%) of respondents indicate that they regularly recruit individuals with current clearances from other contractors. Another 10% say they recruit employees from government with active clearances, and the remaining 36% say they work to clear existing staff without clearances and deploy them to national security related projects. That means that almost two thirds of employees brought on to programs are ripped from another program they are currently working for another contractor or as a government employee. That statistic clearly defines the need to infuse new cleared talent into the pool.

Our survey data also indicates that employees with an active clearance consistently command salaries that are dramatically higher than their colleagues performing the same job without a clearance; according to our results, 56% of respondents noted that they pay premiums of anywhere from 5% to 25% for cleared workers. Perhaps more glaringly, 70% of our respondents indicate that this premium continues to increase as the demand for cleared workers intensifies. In fact, 60% of our survey respondents indicated that they have seen “significant increases” in the contractual requirements for cleared workers over the past 5 years. In a recent GAO report on the DoD clearance backlog, investigators noted “a growing percentage of all DoD requests for clearances is at the top secret level. For example, in fiscal years 1995 and 2003, 17 percent and 27 percent, respectively, of the clearances requests for industry personnel were at the top secret level” (*GAO-04-344 DoD Personnel Clearances report*, page 15). GAO goes on to note that this increase is significant because clearances at the top secret level must be renewed twice as often as secret clearances, and take eight times as long to investigate and three times as long to adjudicate than clearances at the secret level.

Our survey indicates as well that the time to complete clearances continues to rise. We asked our respondents to tell us how long it takes on average for them to obtain a Top Secret clearance. We asked respondents to take into account both the investigative and adjudicative time periods. Seventy percent (70%) of our respondents noted that it takes on average more than 270 days to obtain this level of clearance. We also asked respondents to answer the same question from a perspective of one and two years ago. Fifty-nine percent (59%) indicated

that the process took more than 270 days a year ago, while 49% told us it took longer than 270 days two years ago.

On average, our survey respondents indicated that nearly 60% of their cleared workforce performs duties on DoD-related contracts. No one denies that DoD is the largest single organization that grants clearances to industry personnel. At the same time, the clearance problem is one that affects all agencies of government. Given the enormous scope of DoD's involvement in this function, we understand the demands placed on DoD to clear the enormous number of individuals, but we believe industry and government must work together to implement a workable solution to reduce the time it takes to secure a clearance and increase the portability of clearances across government agencies.

Our survey results reinforced what we in industry already knew: cleared personnel cost more, there is an increasing need for cleared personnel, and industry hire away cleared personnel from one another with great regularity to decrease the risk that a critical program will miss milestones for lack of adequate staff.

ITAA does not believe the problem lies just with DSS and OPM. The problem is exacerbated by antiquated policy that leadership does not want to address. While we applaud the efforts underway to reform the process, similar initiatives have failed in the past because we are trying to automate a system that needs to be re-engineered to address security realities of today. Similarly, there appears to be a disconnect between the procurement functions and the security functions. Procurement officers generally issue security requirements to contractors, and these requirements generally dictate the number of security "billets" a company is required to hold, and the security level for each of those billets. It is great that DSS can issue an interim secret clearance in 3 to 5 days, but the problem is that industry has very few contracts that have been designated at that level. Part of the reform of the security clearance process, we believe, must include an examination of how security clearance levels are set and approved during the procurement phase of a project.

ITAA has led the formation of a diverse coalition of trade associations to develop joint recommendations on how to improve the current process. This coalition has produced a white paper, which I attach to my testimony today and ask to be included in the official hearing record. Joining ITAA on this industry white paper are seven other prominent trade associations that represent the broad spectrum of the government contracting community:

- The Security Affairs Support Association (SASA);
- The Professional Services Council (PSC);
- The National Defense Industrial Association (NDIA);
- The Contract Services Association (CSA);
- The Northern Virginia Technology Council; (NVTC)

- The Armed Forces Communications and Electronics Association (AFCEA); and
- The Electronic Warfare & Information Operations Association, more commonly known as the Association of Old Crows (AOC).

Together, these organizations represent thousands of companies and tens of thousands of individuals with diverse responsibilities across the security and defense spectrum: from IT services, to manufacturing and engineering, and from complex services offerings, to weapons development and modernization. Working together, these industry associations have developed five specific recommendations to improve the security clearance process, improve the nation's security posture, better enable our members to serve their customers, and lower the cost to government. The changes we recommend in this white paper, we believe, would have a significant impact on the ability of people to obtain, hold, and maintain their clearance status and will ensure that critical government programs do not go unexecuted for lack of available cleared personnel. I will present these recommendations in summary form here, as the white paper covers these issues and recommendations in much greater detail, and will also cover some additional issues ITAA has concerns with that are not specifically addressed in the white paper.

SPECIFIC RECOMMENDATIONS FROM ITAA

Much of the debate of late, Mr. Chairman, surrounding the issue of security clearances has focused on the transfer of investigative functions of the Defense Security Service to the Office of Personnel Management that was authorized as part of the FY 2004 Defense Authorization bill. Many have pointed to this authorized transfer as the prescription to solve the long delays and process challenges inherent to this process. As GAO and others have noted, however, the potential transfer has been slow to proceed. Industry is concerned both with the delays in a potential transfer, and with the notion that this transaction will somehow miraculously improve the current process. While there will be advantages in moving to a single case management system at OPM, ITAA believes little will actually change without significant reform of the processes that underlie the current program. Moving the responsibility for investigations from one entity to another will do little to fundamentally change the process.

In fact, we understand that as a result of the impending merger of DSS and OPM, a large number of security clearance investigations submitted to DSS since the start of the fiscal year remain unopened. Of the estimated 100,000 cases in this category, a substantial number represent defense industry personnel. This situation only exacerbates the problems we have identified above in filling vacant contractor positions in a timely manner with cleared personnel. GAO has pointed out that OPM will increase its annual investigative caseload by nearly 800,000 cases when the merger with DoD takes effect. This increase in caseload will tax an already over-burdened system, and industry is

concerned that this situation could result in even greater delays in the issuance of clearances.

As we look to solutions, ITAA believes it is important to support the Office of Management Budget and Office of Personnel Management e-Clearance initiative as a means to reduce backlogs in issuing clearances. While the work done as part of the e-Clearance initiative is helpful in increasing timely access to existing clearances and automating the paperwork requirements to apply for a clearance, we believe much more needs to be done to reform the process and get cleared workers deployed to critical contracts and support functions more quickly. Specifically, ITAA recommends:

- That federal agencies examine issues relating to procurements and recommend corrective actions to allow for 'Bench Strength' on contracts requiring security clearances;
- That data requirements and clearance processes be standardized across federal agencies to provide for uniform baseline standards all agencies recognize for like levels of clearances;
- That reciprocity (or crossover) for clearances from agency to agency be dramatically increased so like clearance levels can be applied to any agency in government;
- That agencies work with the private sector to address the current investigative and adjudication backlog by employing a coordinated approach that leverages private sector expertise and information technology to speed investigations and adjudications. Specifically, we recommend that government examine the use of commercially available databases to reduce investigative demands and establish on-going monitoring for adverse events to reduce the need for periodic reinvestigations;
- That Congress request the Defense Science Board to immediately review policies governing security clearances and make recommendations for changes, including recommendations on changes in the procurement-related aspects of clearance requirements; and
- That Congress support and fully fund OMB's and OPM's e-Clearance Initiative.

We believe that the changes recommended here would have a significant positive impact on the ability for people to obtain, hold, and maintain their clearance status. And we believe that an improved process would open new opportunities for people seeking employment in sensitive private sector specialties.

The recent stand-up of the Department of Homeland Security presents new opportunities to address how this process functions at a new agency during its foundational stages. As DHS continues to integrate the operations of the 22 disparate legacy agencies that comprise it, we have a good opportunity to fix

what's wrong before the process gets too ingrained in the culture of the Department. The process so far within DHS has been slow, but I think everyone in the contracting community is willing to give DHS more time to deal with the issue given their nascent stage. It's important to note, however, that in their brief time of existence, the clearance issue has been raised in several instances in the context of other oversight hearings. At a hearing of the House Select Committee on Homeland Security last year, for example, witnesses testified about significant delays in the granting of security clearances to airport screeners and state and local first responders. ITAA's membership also fulfills critical services for this community and has significant concerns about how delays in granting clearances for contractor personnel affect this unique community. Access to a government-wide clearance database like the Joint Personnel Adjudication System (JPAS) and full implementation of security clearance reciprocity would reduce the time first responders wait to obtain clearances and make it easier for these critical components of our national security to work in better collaboration with the federal government. Faster clearance times would also ensure that contractor personnel supporting critical first responder missions receive timely classified information that is transmitted to the user community.

AGENCIES SHOULD ALLOW FOR “BENCH STRENGTH” ON CONTRACTS REQUIRING SECURITY CLEARANCES

The current clearance process across all agencies requires that clearances be granted only to those currently assigned to projects or contracts requiring a clearance. Industry would recommend that agencies be permitted to clear up to 20% of additional industry personnel. Under most contracts, industry is told how many billets they need to fill by way of the RFP or information received from contracting officers. Many federal security officers report that they are then constrained by the number of billets allocated by a contracting officer to a particular contract. If an individual leaves the company that has that contract, or the company needs to rotate that person to another contract they are working on, a slot opens up on the contract that needs to be filled. Unless the company has a ready staple of cleared personnel who can immediately step in at that particular agency at the correct clearance level, the company is usually forced to start the process for a new employee all over again. ITAA recommends that agencies move toward allowing bench strength by first educating the procurement workforce across the government on the critical issues that arise from the limited cleared slots currently provided for in federal contracts.

Providing for bench strength would bring benefits to government and industry in that the increased supply of cleared people would bring down the cost to government and industry would be able to ensure the best people are working a project as opposed to only those who simply “hold a clearance.” The creation of 'bench strength' of cleared people would also enhance national security, as there would be a pool of individuals readily available to address critical missions. We

believe this is also a critical requirement to limit the spiraling salaries of employees with clearances, a cost that ultimately is paid by the government.

An additional consideration is the aging government workforce. As these seasoned government workers retire, even more demands will be placed upon contractors to supply cleared quality personnel. Industry would be willing to look into sharing the cost of creating this bench strength, following the precedent of paying for expedited investigations at the National Security Agency (NSA).

GOVERNMENT SHOULD STANDARDIZE DATA REQUIREMENTS AND INVESTIGATIVE PROCESSES FOR LIKE SECURITY CLEARANCES

All security clearance processes ultimately assess a core set of investigative data. For example, most clearance processes examine a subject's identity data, address history, employment history (including military service record), educational achievement, financial status, and personal references, with the additional requirement for a National Agency Check for derogatory information (i.e., criminal history, intelligence or other government data) that would increase risk. The commonality of the data required for clearances creates the opportunity to standardize collection and assessment of that data across the government.

ITAA envisions that the standardization process would start with identifying data elements and investigation processes common to all clearances to set a "baseline" background investigation. That baseline could then provide the foundation for a tiered structure of security levels to correlate to the level of trust required and consequences of a breach of trust for categories of missions, operations, functions or facilities. The government could accommodate different levels of security by varying the breadth and depth of the investigation or the rigor of the adjudication criteria, as well as assessing additional elements of the applicant's background beyond the baseline.

The baseline, however, would apply as the minimum standard for the lowest level security clearance in the context of any government operation – civilian, defense or intelligence. Higher levels of clearance would require a more intensive inquiry (e.g., longer historical perspective, polygraph) or assessment of additional elements of the subject's background (e.g., "life style" queries). Standardizing data and process requirements at each tier for clearance levels across operations with common risk profiles (i.e., law enforcement, homeland security, defense, intelligence, etc.) across the government would yield tremendous efficiencies to reduce time and cost of administering clearances while increasing the effectiveness in maintaining security.

Establishing a common baseline would also reduce the need for multiple application, investigation and adjudicatory processes, which in turn would minimize requirements for specialized training and certification of investigators and adjudicators. Standardization also would facilitate implementation of the

OMB/OPM e-Clearance initiative and promote centralized administration of clearance information government-wide.

At the same time, industry believes that by granting immediate access to industry to databases like DoD's JPAS and the Office of Personnel Management's Clearance Verification System (CVS), industry can make quantum leaps in its ability to quickly and efficiently transfer clearances with little or no cost or delay. Currently, when an employee leaves ABC Company to go to work for XYZ Company it can take over four weeks, as contractors wait for a government agency to transfer for the paperwork between parties. A common database approach like JPAS/CVS will ensure that each agency is able to effectively share clearances in the fastest possible manner. DSS has begun this process with the larger firms and is now making its way to small businesses.

In addition to efficiencies in the initial clearance process, standardization would facilitate transferability and ongoing administration of clearances from one agency to another or even across levels of government. Operating from a standard baseline would streamline and expedite the process of adjusting clearance levels or clearing individuals for new missions by enabling investigators to focus only on updating the baseline and/or evaluating additional elements beyond the baseline as opposed to repeating the entire process from scratch. In addition, development of standard structure of security clearance requirements could some day facilitate a system to monitor the continuing validity of clearances. The government could enroll all individuals holding a specified clearance in a database to monitor available public and government records for changes in status (e.g., arrest, bankruptcy, unexplained affluence, etc.) that might indicate a potential security risk.

In fact, the DoD has developed and tested such a system, the Automated Continuing Evaluation System (ACES), which is low cost and can be deployed in six months if final funding is approved. The ACES monitoring system, using advanced techniques, will identify and flag specific risk factors as defined in the applicable security rules based on near real-time searches of approximately two-dozen government and commercial databases.

Early deployment of ACES would provide the government with much earlier and cost effective warning of potential security issues than the current reinvestigation process alone, and would also reduce reinvestigation time, thereby freeing up resources to pursue investigative functions on new clearances. Standardizing clearance criteria and processes with an ongoing monitoring process, along with an accurate and reliable clearance database, will enable security officials to have greater confidence in clearances conducted for other agencies, facilitating transfer and acceptance of security clearances across the government.

In four Departments and agencies within the intelligence and defense community that we examined, we found four different standards and processes for

clearances. Industry would recommend that the process be reconciled between the largest organizations. At an absolute minimum, industry would propose that the DOD, NSA, CIA, and NRO work to reconcile their data requirements and processes for investigations and adjudication in line with the recommendations made above. In conjunction with a statutory performance metric to get clearances issued within 120 days, we would recommend the appointment of a joint working group to develop standardized processes across the government. We believe that industry should be represented on this panel as well. ITAA believes that another potential solution would be to task the Defense Science Board to present specific recommendations to the Secretary of Defense on how to improve the current process. The last thing we need is another study on the problems we're facing. What we need are solutions, and as you know Mr. Chairman, the Defense Science Board's recommendations are actionable.

GOVERNMENT MUST PROVIDE FOR INCREASED RECIPROCITY FOR CLEARANCES ACROSS FEDERAL DEPARTMENTS AND AGENCIES

Much like the lack of standardization in clearance requirements, there is currently little reciprocity among federal agencies to honor a clearance granted by another federal Department, even when at the same level. It would seem rational to argue that when one federal agency grants you a top-secret clearance, that clearance should be honored by any other government agency that requires you to have clearance at the same level, provided the investigation remains current. Sadly, however, this goal is hardly ever realized, despite the existence of Executive Orders from multiple administrations requiring greater standardization of criteria and portability. Even within individual government agencies we've found unique processes for clearances at the same levels. In fact, examples of intra-Departmental battles over clearance levels abound; within the Department of Justice prior to the stand-up of DHS, for example, a clearance held at the Drug Enforcement Administration might not be honored by the Federal Bureau of Investigation, and vice versa, because of different criteria to get those clearances.

ITAA has identified more than 20 distinct processes across the federal government; each process has its own special requirements that go beyond or are unique from other agencies. These requirements prohibit one agency from honoring the same level of clearance from another agency. ITAA would recommend that a baseline requirement be created by the advisory body we recommend above to indicate that in accordance with uniform standards, no federal agency will reinvestigate an individual who holds an active clearance at the required security level from any other federal agency, again, provided that the investigation is current. While there may be additional criteria to be examined, the baseline level of clearance should be accepted and agencies shouldn't repeat an entire investigation on someone who has undergone the same review for another agency.

Industry would also like to have authority to transfer clearances between each other on a near real-time basis. This relates to the situation when an employee leaves ABC Company to go to work for XYZ Company. Member firms of the ITAA coalition have documented that this simple process varies dramatically by agency, and can take over four weeks, as contractors wait for a government agency to transfer the paperwork between parties. A common standard and approach to sharing clearances should be developed to ensure that each agency has the same standards and is able to effectively share clearances in the fastest possible manner.

GOVERNMENT MUST ADDRESS THE CLEARANCE BACKLOG BY PARTNERING WITH INDUSTRY AND LEVERAGING INFORMATION TECHNOLOGY TO IMPROVE PROCESSES AND MANAGEMENT

ITAA certainly applauds the growing use of private sector investigative providers to help conduct background investigations; however, even with the use of the private sector, the increased numbers of clearances being requested is extending the backlog that already exists and resulting in even longer delays at both the investigative and adjudicative ends of the process. Based upon our member's experience, there is an increasing adjudicative backlog as more investigations are being completed and overwhelming the available adjudicative workforce. In its recent report to the Armed Services Committee, GAO pegged the current backlogs at DoD alone at nearly 360,000.

Information technology has transformed government services in countless ways. As we continue the e-Government revolution that has already modernized so many antiquated government programs, ITAA believes that the power of information technology can do much to improve this vital process as well. In addition to recommending support for existing e-Government initiatives, ITAA also would note that reliable commercially available technologies like public records databases can play a vital role in verifying information submitted by applicants for clearances. Several highly respected companies already support major corporations in their employment pre-screening and risk management processes by offering databases that can help verify whether an individual has had financial problems such as liens or judgments, whether the individual has a criminal history that would disqualify them from receiving a clearance, and whether the individual in fact lived at a location they claim on an application. These applications can dramatically reduce the need for field agents to spend valuable time pounding the pavement interviewing friends and co-workers of the individual under investigation. Clearly the role of field investigators cannot be done away with; there is vital information discovered in personal interviews with subjects who know an individual well. We do believe, however, that the power of information technology can vastly improve the length of this process without compromising security.

IMPLEMENT/FUND THE OFFICE OF PERSONNEL MANAGEMENT'S E-CLEARANCE INITIATIVE

ITAA endorses the Office of Personnel Management's (OPM) e-Clearance initiative. The concept of e-Clearance, such as sharing resources on-line, whether for information collection, information review, or adjudication, including sharing among interested agencies, can help transform and speed the clearance process by reconciling and harmonizing the existing disparate clearance procedures. While the automation of standard clearance forms and the establishment of a central database of existing clearances should help the process, the coalition recommends that the e-Clearance initiative also address the shared data and process issues identified in our testimony. We recommend that Congress provide full funding and support for the e-Clearance initiative in annual appropriations.

Conclusion

I cannot emphasize enough Mr. Chairman that industry is committed to preserving the strict requirements to obtain security clearances. The coalition's interest is not to minimize current requirements, but rather, to make sensible and positive changes to an antiquated process and policy that would allow the nation to maintain strong vigilance on who has access to data, while better serving the defense and intelligence communities at the lowest possible total cost. Involving the Defense Science Board to review and make recommendations to this problem would be a good first step. Industry looks forward to working with the government to examine and implement the recommendations we make today to move the average top secret clearance form 12 months to 120 days. We stand ready to devote our experience and significant expertise with best practices to ensure that critical government programs do not go unexecuted for lack of available cleared personnel, and we look forward to growing our companies by adding many new employees with highly skilled and compensated new jobs. Thank you Mr. Chairman for the opportunity to appear before the Committee today. I would be happy to answer any questions from you or other members of the Committee.

Improving the Security Clearance Process Through Automation and Common Criteria:

A White Paper on Issues Confronting the Government Contractor Community

Prepared by

Information Technology Association of America
Professional Services Council
Security Affairs Support Association
Contract Services Association
Armed Forces Communications and Electronics Association
National Defense Industrial Association
Northern Virginia Technology Council
Association of Old Crows





NORTHERN VIRGINIA
TECHNOLOGY COUNCIL

EXECUTIVE SUMMARY

The federal government continues to rely heavily on commercial industry partners to fulfill critical government services. Recent studies have suggested that as many as 850,000 government jobs are commercial in nature. The magnitude of commercial activities necessitates that government and industry work together to ensure the best private sector personnel are available to fulfill critical government services. In order to perform many critical services, industry personnel must obtain and renew security clearances. The current security clearance process, rules, and regulations are very important to industry and create a mechanism that we believe must be improved upon in order to better safeguard the national security by permitting industry to obtain and clear qualified personnel in a timely fashion. Industry faces increased pressure to deliver cleared personnel on the day a contract begins, and the current delay in obtaining security clearances increases costs to the federal government by delaying the introduction of the best personnel to critical programs.

Elongated clearance processes adversely affect mission accomplishment, keep people from working in a productive and timely manner, and add to the cost of contractor programs to the federal government. Members of several industry associations have developed four specific recommendations to improve the security clearance process, improve the nation's security posture, better serve our customers, and lower the cost to government. The changes recommended here would have a significant impact on the ability of people to obtain, hold, and maintain their clearance status and will ensure that critical government programs do not go unexecuted for lack of available cleared personnel.

With the growing backlogs and investigative delays being experienced by the Intelligence Community, Defense Security Service and the Office of Personnel Management, it can take more than a year to process a new employee for a background investigation and a security clearance. Even new employees with prior investigations and security clearances can wait weeks for their clearance to be converted or reinstated by the government. While all this "lost" time is not completely non-productive, in some cases the employee cannot be of full value to the contract and customer without his or her final security clearance; in most cases, it prevents the hiring of qualified people.

BACKGROUND

The Information Technology Association of America (ITAA) along with partner organizations including the Professional Services Council (PSC), Security Affairs Support Association (SASA), Contract Services Association (CSA), Armed Forces Communications and Electronics Association (AFCEA), Northern Virginia Technology Council (NVTIC), National Defense Industrial Association (NDIA), and

the Association of Old Crows (AOC) (collectively, “the coalition”) present this paper on the current state of the security clearance process for contractors. The collective membership of these organizations is drawn from the leading technology firms in the United States. These companies develop and deploy the technology products and services that have helped to make the United States’ intelligence and war fighting capability the best in the world.

In order to serve their defense and intelligence clients, our members are required to obtain appropriate security clearances for their facilities and employees. The security clearance process, rules, and regulations are of vital interest to industry and create a process that we believe must be improved upon in order to better safeguard the national security. While much has been done since the Eisenhower administration in both policy and procedural areas to try and standardize and simplify the government’s personnel security program and promote the notion of clearance reciprocity, in practice it has simply failed to achieve the stated goals and objectives, leaving industry to the mercy of a diverse bureaucracy that is slow to embrace change and eager to protect its “rice bowls.” Industry faces increasing pressures to deliver cleared personnel on the day a contract begins, and the current delays in obtaining security clearances limits competition and increases costs to the federal government by delaying the introduction of the best personnel to vital programs and slowing the initiation of critical programs.

As the Bush administration seeks to provide greater competition with the private sector to perform functions inherently commercial in nature, it is critical that the current clearance process be streamlined and improved. The elongated clearance process is delaying missions from being completed in a timely fashion, keeping people from working, and adding to the cost of contractor programs to the federal government. In today’s clearance process, it is virtually impossible to share a good idea or leverage an existing team between agencies. It is unknown what the total current number of cleared contractor job vacancies is across government, but one program alone at NSA is said to have more than 400 openings. The current clearance process prevents thousands of vacant positions requiring a security clearance from being filled in a timely manner. Given the critical role that the Intelligence Community agencies play in securing the national security of the United States, we must fill these and other critical positions with cleared, skilled people as soon as possible. The post September 11th increase in the need to clear and hire staff in all agencies has added to the investigative and clearance backlog problem and we must conclude that a considerable amount of important work is not getting done. While the agencies strive to fill these critical positions, programs requiring cleared contractor personnel suffer as a result of growing investigative and clearance backlogs as well as bureaucratic impediments and opposition to implementation of clearance reciprocity policies that were enacted in Executive Order 12968 following the Ames espionage case.

Recent studies conducted under the Federal Activities Inventory Reform (FAIR) Act suggest that as many as 850,000 government jobs are commercial in nature. The magnitude of commercial activities necessitates that government and industry work together to ensure the best private sector personnel are available to fulfill critical government services.

RECOMMENDATIONS

In principle, the coalition supports the Office of Management and Budget's and Office of Personnel Management's e-Clearance initiative as a means to reduce backlogs in issuing clearances. There are also four recommendations that we believe will improve our security posture, better serve our customers, and lower the cost to government. These are:

- That agencies allow for 'Bench Strength';
- That agencies address the current investigative and adjudication backlog,
- That there be increased reciprocity for clearances from agency to agency; and
- That data requirements and clearance processes be standardized across agencies.

We believe that the changes recommended here would have a significant positive impact on the ability for people to obtain, hold, and maintain their clearance status. An improved process would open new opportunities for people seeking employment in sensitive private sector specialties; as recently documented in one *Washington Post* article, a northern Virginia contractor has over 70 openings but can't fill the positions due to a lack of cleared people or the cost to the company of hiring and waiting up to eighteen months for their clearances to come through.

A July 2003 hearing of the House Select Committee on Homeland Security also uncovered significant delays in the granting of security clearances to airport screeners and state and local first responders. The coalition's membership also fulfills critical services for this community and has significant concerns about how delays in granting clearances for contractor personnel affect this unique community. Access to a government-wide clearance database and full implementation of security clearance reciprocity would reduce the time first responders wait to obtain clearances and make it easier for these critical components of our national security to work in better collaboration with the federal government. Faster clearance times would also ensure that contractor personnel supporting critical first responder missions receive timely classified information that is transmitted to the user community.

Since the current process dictates that security clearances can be held only by individuals who have a bona fide need for access and are employed in a job requiring a security clearance, the Government's process is collectively reducing the supply of cleared staff at a time when the need is increasing. This supply and demand effect is resulting in large increases in salaries of people holding clearances and cleared personnel are moving between employers that are anxious to fill agency openings with cleared people. Because of the costs associated with obtaining security clearances, currently cleared personnel command salaries on average 5% to 10% higher than those for non-cleared

personnel according to industry estimates. This cost is most often passed on to the government.

The recommendations from the coalition are detailed below to improve processes to greater benefit the missions of our customers and the security of the United States.

One agency CIO recently commented that the current security process has created a “pseudo society” of people: “These people remain employed not because they work hard, bring innovation, or have the most current skills. They are maintained and even bestowed gracious pay and perks because of their clearance. We need to eliminate this pseudo society and make their contribution the most important factor.”

ALLOW FOR “BENCH STRENGTH”

The current security process across all agencies requires that clearances be granted only to those currently assigned to projects or contracts requiring a clearance. Industry is recommending that agencies be permitted to clear additional industry personnel, up to 20 percent of their current cleared population. This would bring benefits to government and industry in that the increased supply of cleared people would bring down the cost to government and industry would be able to ensure the best people are working a project as opposed to only those who simply “hold a clearance.” The creation of ‘bench strength’ of cleared people would also enhance national security, as there would be a pool of individuals readily available to address critical missions. We believe this is a critical requirement to limit the spiraling salaries of folks with clearances, a cost that ultimately is paid by the government.

While the coalition understands that increasing currently cleared personnel may increase investigative and adjudication workloads in the short-term, increasing the supply of cleared resources will benefit the government in three ways. First, it will increase supplies and lower costs long term. Second, the ability for a new or expanded project to get underway quickly will be immensely enhanced. Lastly, an increased pool of resources will make it easier to place quality personnel; it will be much easier to replace people in particular and contractors in general if a larger supply of cleared resources exists.

An additional consideration is the aging government workforce. As these seasoned government workers retire, even more demands will be placed upon contractors to supply cleared quality personnel. Industry would be willing to look into sharing the cost of creating this bench strength, following the precedent of paying for expedited investigations at NSA.

ADDRESS THE ADJUDICATION BACKLOG

While the coalition applauds the growing use of private sector investigative providers to help conduct background investigations, we are seeing an increased delay in adjudication timelines. Adjudication, until relatively recently, has been considered an inherently governmental function. Based upon our member's experience, there is an increasing adjudicative backlog as more investigations are being completed and overwhelming the available adjudicative workforce. Based on successful outsourcing of adjudicative support functions in the Department of State, Department of the Navy and BCIS (former INS) the coalition recommends that the government make greater use of contract adjudicator support functions until backlogs are eliminated and clearances can be issued or reinstated in 30 days or less.

INCREASED RECIPROCITY FOR CLEARANCES

There is currently little reciprocity of security clearances in the federal government. This is one reason why there is little sharing of information and best practice ideas across the community. Lack of sharing clearances prevents the best and brightest serving one agency to quickly move to solve a similar problem at a different agency.

The coalition would like to create a process where they are allowed to easily move people in a shared clearance process. The lack of sharing between agencies causes problems for employee and employer when a project comes to an end. Once a person is 'read off' of an agency and there is no immediate need for him/her to have a clearance then it is likely they will lose this clearance. If they need to go back to the agency or are transferred to work at another agency a few weeks later, the reinstatement or reinvestigation can take months. With greater sharing there is a much better chance the employee could be moved to another cleared project supporting a different agency.

Similarly, industry would like to be able to have authority to transfer clearances between each other. This is the situation when an employee leaves ABC Company to go to work for XYZ Company. Member firms of the coalition have documented that this simple process varies dramatically by agency, and can take over four weeks, as contractors wait for a government agency to transfer for the paperwork between parties. A common standard and approach to sharing clearances should be developed to ensure that each agency has the same standards and is able to effectively share clearances in the fastest possible manner. The benefits of this approach would also improve the ability of our nation's first responders to work with federal agencies.

Standardize Data and Processes for Like Security Clearances

While security clearance processes vary across the government with different missions, operational, functional and policy requirements, all of the processes ultimately assess a core set of investigative data. For example, most clearance processes examine a subject's identity data, address history, employment history (including military service record), educational achievement, financial status, and personal references with the additional requirement for a National Agency Check for derogatory information (i.e., criminal history, intelligence or other government data) that would increase risk. The commonality of the data foundation for clearances creates the opportunity to standardize collection and assessment of that data across the government.

The standardization process would start with identifying data elements and investigation processes common to all clearances to set a "baseline" background investigation. That baseline would provide the foundation for a tiered structure of security levels to correlate to the level of trust required and consequences of a breach of trust for categories of missions, operations, functions or facilities. The government could accommodate different levels of security by varying the breadth and depth of the investigation or the rigor of the adjudication criteria as well as assessing additional elements of the applicant's background beyond the baseline. For example, the baseline would apply as the minimum standard for the lowest level security clearance in the context of any government operation – civilian, defense or intelligence. Higher levels of clearance would require a more intensive inquiry (e.g., longer historical perspective, polygraph) or assessment of additional elements of the subject's background (e.g., "life style" queries). Standardizing data and process requirements at each tier for clearance levels across operations with common risk profiles (i.e., law enforcement, homeland security, defense, intelligence, etc.) across the government would yield tremendous efficiencies to reduce time and cost of administering clearances while increasing the effectiveness in maintaining security.

Establishing a common baseline would reduce the need for multiple application, investigation and adjudicatory processes, which in turn would minimize requirements for specialized training and certification of investigators and adjudicators. Standardization also would facilitate ongoing initiatives to implement an "e-clearance" process and promote centralized administration of clearance information government-wide, i.e. JPAS/CVS. Increasing sharing of clearance information and reducing the time and resources required to complete low level clearances will enhance security by enabling the government to allocate more of its limited investigations and adjudication resources to clearances with the greatest sensitivity and highest priority.

By granting immediate access to industry to databases like DoD's Joint Personnel Adjudication System (JPAS) and the Office of Personnel Management's Clearance Verification System (CVS) the coalition believes a quantum leap in industry's ability to quickly and efficiently transfer clearances with little or no cost or delay involved will result. Currently, when an employee leaves ABC Company to go to work for XYZ Company it can take over four weeks, as contractors wait for a government agency to transfer for the paperwork between parties. A common database approach like JPAS/CVS will ensure that each agency is able to effectively share clearances in the fastest possible manner. The benefits of this approach would also improve the ability of our nation's first responders to work with federal agencies.

In addition to efficiencies in the initial clearance process, standardization would facilitate transferability and ongoing administration of clearances from one agency to another or even across levels of government. Operating from a standard baseline would streamline and expedite the process of adjusting clearance levels or clearing individuals for new missions by enabling investigators to focus only on updating the baseline and/or evaluating additional elements beyond the baseline as opposed to repeating the entire process from scratch. In addition, development of standard structure of security clearance requirements could some day facilitate a system to monitor the continuing validity of clearances. The government could enroll all individuals holding a specified clearance in a database to monitor available public and government records for changes in status (e.g., arrest, bankruptcy, unexplained affluence, etc.) that might indicate a potential security risk. In fact, the DoD has developed and tested such a system, the Automated Clearance Evaluation System (ACES), which is low cost and can be deployed in six months if final funding is approved. The ACES monitoring system, using advanced data-mining techniques, will identify and flag specific risk factors as defined in the applicable security rules based on near real-time searches of approximately two dozen government and commercial databases. Early deployment of ACES would provide the government with much earlier and cost effective warning of potential security issues than the current reinvestigation process alone, and would also reduce reinvestigation time, thereby freeing up resources to pursue investigative functions on new clearances. Standardizing clearance criteria and processes with an ongoing monitoring process, along with an accurate and reliable clearance database, will enable security officials to have greater confidence in clearances conducted for other agencies, facilitating transfer and acceptance of security clearances across the government.

In four Departments and agencies examined by the coalition within the intelligence and defense community, we found four different processes for clearances. Given that there are more than 20 agencies and departments that require clearances, there are likely 20 unique processes. Industry would recommend that the process be reconciled between the largest organizations.

Industry would propose that, at a minimum, the DOD, NSA, CIA, and NRO work to reconcile their data requirements and processes for investigations and adjudication in line with the recommendations made above.

IMPLEMENT/FUND THE OFFICE OF PERSONNEL MANAGEMENT'S E-CLEARANCE INITIATIVE

The coalition endorses the Office of Personnel Management's (OPM) e-Clearance initiative. The concept of e-Clearance, such as sharing resources online, whether for information collection, information review, or adjudication, including sharing among interested agencies, can help transform and speed the clearance process by reconciling and harmonizing the existing disparate clearance procedures. While the automation of standard clearance forms and the establishment of a central database of existing clearances should help the process, the coalition recommends that the e-Clearance initiative also address the shared data and process issues identified in this paper.

Conclusion

It cannot be overstated that industry is committed to preserving the strict requirements to obtain security clearances. The coalition's interest is not to minimize current requirements, but rather, to make changes to an antiquated process that would allow the nation to keep vigilance on who has access to data, while better serving defense and intelligence at the lowest possible cost. Industry looks forward to working with the government to examine and implement the recommendations made in this white paper, 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.