STATEMENT
OF
MR. TIMOTHY R. SAMPLE
PRESIDENT
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
TO
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE AND THE DISTRICT OF COLUMBIA

Evaluating Progress and Identifying Obstacles in Improving the Federal Government's Security Clearance Process

May 17, 2007

Chairman Akaka, Mr. Voinovich, and Members of the Committee, I am honored to be in front of you this morning to discuss this vitally important issue. I commend the subcommittee for taking on this task, as I believe the personnel security clearance process is at the core of several issues that go well beyond whether an individual should have access to classified information. In fact, the personnel security process and the security culture upon which it is based is responsible for fueling government acquisition processes that unnecessarily cost the government and the American taxpayers billions and for our inability to get the most desired and needed individuals into key positions in government. It was also an important factor in the government's inability to share intelligence between agencies and departments prior to the terrorists' attacks on September 11, 2001.

Mr. Chairman, I am the President of the Intelligence and National Security Alliance (INSA), which is a non-profit, non-partisan, professional association that focuses on a variety of issues related to national security, especially issues confronting our intelligence capabilities. Although the bulk of our membership is based on corporate contributions, INSA is not a trade association – we do not lobby on behalf of a certain set of companies or for specific programs. Instead, INSA operates as a public policy forum aimed at educating government and the public about key issues confronting our national security structures and capabilities. We utilize our individual and corporate membership to access a wealth of expertise and expand our networks in order to provide the best insight and advice to government agencies and to the American people. In general, INSA advocates for strong, robust intelligence capabilities in order to ensure our nation's security. It is with this in mind that INSA, and its Council on Security and Counterintelligence, has studied the issues that the Committee is confronting today. Our experience stems from the network of expertise found in our Council as well as from a

history of study from our predecessor organization, the Security Affairs Support Association (SASA). The INSA Council on Security is in the process of completing a white paper on the need to transform the personnel security clearance process. Several of my remarks come from our assessments. I will send copies of this white paper to the Committee once completed, and I hope that you will consider its points in your overall deliberations. With this background in mind, let me turn to the issues at hand.

Mr. Chairman, you have chosen to title this hearing: *Evaluating Progress and Identifying Obstacles in Improving the Federal Government's Security Clearance Process.* I will structure my remarks to respond to these two issues you raised: how have we progressed in our security clearance procedures, and what are the obstacles to improving our security processes? As I will detail throughout my remarks below, despite recent attempts at reform, there has been no appreciable difference in the security clearance situation. One need only look at the average clearance processing times, even the cheery and creatively calculated averages, to see that the backlog and processing times have not improved, and perhaps worsened, during this decade.

In response to the question of obstacles to improvement, we agree with the Security Clearance Reform Coalition's (of which we are a member) conclusions that technology needs to be employed in the process, agencies must stop crafting their own requirements for mutual recognition of clearances, among others. We can add more obstacles to this list, including an outdated field investigation; agencies that refuse to honor other agencies' equivalent clearances; and clearances that are tied to agencies as opposed to the individual.

At a minimum, Congress should strongly consider implementation of the Coalition's recommendations. But in doing so, you must understand that you end up with a more efficient flawed system. Although these improvements are important, they are not sufficient to fix the root cause of this broken system: a culture steeped in risk avoidance. As I will explain further, this culture of risk avoidance causes an immense backlog of initial clearances, neglects the re-investigation process of cleared personnel, and incentivizes security officers against clearing first and second generation Americans and those with extensive foreign travel and contacts, despite overwhelming evidence that those individuals have the expertise our intelligence community and government desperately need.

Evaluating Progress in the Security Clearance Process

Invariably, recent discussions about security clearances focus on the issues of the backlog of individuals awaiting clearances, which number in the hundreds of thousands, and the time it takes to "clear" them. Congress itself, in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), focused on such numerical measures of merit when it directed that government agencies achieve average timelines of 90 days for investigations and 30 days for adjudication for 80 percent of all initial clearances.

Although I would strongly urge the Committee to go well beyond these two data points – as I will later in this testimony – I would like to start with these areas of debate.

First, a testament to the inefficiencies of the current process is that valid metrics cannot be derived due to the lack of transparency within the system, the lack of compatible systems between and among agencies and departments, the fragmented nature of the process, and the intensity of manual labor demanded by the current processes. As a result, so-called authoritative numbers that are delivered by the Office of Personnel Management (OPM), the Government Accounting Office (GAO), the Department of Defense (DoD), or other entities must be considered to be like political polling numbers – highly subject to interpretation depending on what outcome is desired. The September 2006 GAO report on DoD Personnel Clearances provides a prime example: the appendices contain letters written by OPM and OMB disputing the methods and calculations in the report.

This is not meant as a criticism of those presenting the data, as much as recognition that the current process does not allow for valid, unbiased empirical data to be collected. OPM's Security Clearance Oversight Group report in February of this year projected timelines suggesting that IRTPA investigation and adjudication goals will be met this year by OPM, while the recent GAO report stated the OPM averages 446 days was required for initial clearances, far above IRPTA's mandated 120 day average. In considering the OPM report's data, we note what is not considered in the evaluations. Specifically, the report notes that the timelines do not consider the application process – that is the time from when an individual fills out the necessary forms until the "case file" is declared ready for investigation by the investigative agency. This is a critical aspect of the investigation in that many cases have significant delays if the application data is incomplete or if all the data doesn't arrive into the case file due to the extent of reliance on a very manual process. Moreover, your constituents awaiting clearances don't care which part of the process is considered in these goals and evaluations. They just know that they continue to wait an unreasonable amount of time to get a clearance and go to work.

The report also notes that the reinvestigations are not addressed. This is because the main focus of agencies, and of Congress, since September 11, 2001 has been on obtaining initial clearances for the large numbers of new government employees and contractors required. This is specifically important because, by focusing government efforts on initial investigations, significant security risks are being created by a growing backlog in periodic reinvestigations. In fact, the recent GAO report indicates that the average timelines for reinvestigations are now up to 545 days. Consequently, although the government has attempted to improve some aspects of the existing process, the results are marginal and misleading.

Identifying Obstacles in the Security Clearance Process

Today, the personnel clearance process that we utilize in government and industry is not that different from when it was implemented some 60 years ago. The security clearance process relies on a front-end investigation and, once cleared, the individual is not regularly re-investigated for at least five years. All agencies follow investigative and adjudicative standards established by a series of laws and executive orders, but many have additional agency-specific policies and processes, increasing the difficulty in reciprocity. Furthermore, the field investigation process is less effective than it once was. Although some pieces of valuable information can be discovered in some cases during an investigation, our society has changed to the point that in most cases more information about you can be derived from available databases than from asking your neighbor whether or not you live within your means.

Overall, this current process can be referred to as "risk avoidance," whereby thorough investigations of individuals are conducted prior to allowing them access to classified information. We refer to it as risk avoidance because the emphasis is placed on the initial vetting. Does the candidate have bad credit or a drinking problem? Does the candidate have extensive foreign contacts or a mental disorder? While none of these factors individually or together guarantees that an individual will misuse, sell, or give away our nation's secrets, the risk avoidance process argues that if an individual initially passes these criteria, they are less likely to do so. The "risk avoidance" process flourished and arguably adequately protected our nation's secrets, albeit with some notable, damaging exceptions.

The risk avoidance culture and system has some damaging repercussions for security and counterintelligence today. First and foremost, the emphasis is placed on the initial investigation, but not nearly enough on the monitoring or reinvestigation of those who already have access to classified information. This is a dangerous oversight. The most high-profile spy cases of the past 15 years have been committed by those who have had access to classified information for decades, not those who just got in the door. Ana Montes worked for the DIA for 16 years when she was caught spying for Cuba; Robert Hanssen had 25 years at the FBI. Aldrich Ames worked for the CIA for 23 years before he walked into the Soviet Embassy in Washington and offered to spy against the United States, which he did for nine years before his capture in 1994. All three spied under the same system we are evaluating today.

Individuals with security clearances are nominally reinvestigated every five years, a term that is becoming longer because of the backlog. Because of this focus on initial clearances, we are creating inherent security risks by taking away critical resources that currently make up our principal capability of revealing breaches in security at an individual level. Because of this, it is, unfortunately, not unreasonable to contemplate that another Ames, Montes or Hanson might be able to continue spying while their reinvestigation is caught up in the clearance backlog.

A second outcome of the risk avoidance culture is our inability to get the right people in the right job when we need them. As I mentioned before, our risk avoidance security culture discourages hiring first and second generation Americans for classified

positions because they have foreign contacts, such as family living in a foreign country. While everyone seems to agree that these individuals have the language skills and cultural understanding that are vitally important in today's world, our risk avoidance security culture dictates that these individuals are too risky to be granted access to classified information. It is a sad reality that, even in this era of global business and world-wide terrorism, our security process is highly slanted to hire individuals who have read a book about a country than someone who has actually been there. Put another way, with the philosophy of today's security clearance process, we likely would not hire those individuals who were so critical in breaking Japanese codes in World War II or building the atomic bomb.

The impact on industry supporting government is also substantial. Private sector contractors have a difficult time filling positions that the government requests. The government's security and acquisition processes have created a market in which a contractor is almost forced to hire personnel based on whether he or she has clearance, rather than supplying the best possible candidate. Ultimately, industry then charges the costs engendered because of these issues back to the government, driving up government contract costs well beyond what should be necessary.

In order to meet the requirements of today's acquisition process, industry must hire individuals for specific contracts and then submit them for clearances should they win the contract. This means that industry must not only have someone on their books for over a year, but they must find these individuals something to do while they wait. In some cases, there may be other, unclassified, contracts on which they can work. If not, these individuals get assigned "busy work" and are paid out of companies' overhead funds. In other cases, the individual may leave the company before contract award because they have found more meaningful work with some other company that can put them to work right away. In still other cases, industry will only bid "cleared" individuals in their employment with the hope of being able to replace them with new individuals as those individuals' clearances are finally granted.

The second aspect of the impact of the current process is that a premium has now been placed on hiring individuals with security clearances. In some cases, significant bonuses and a salary structure that can be up to 35% higher than someone without a clearance have been experienced. Consequently, the competition to entice an individual from one company to another, or from government to a company, is intense. The results can be an unstable government workforce as well as an unstable acquisition process as programs experience a revolving door of individuals throughout the period of performance.

The Solution: A New Security Paradigm

Mr. Chairmen, I have outlined for you a few of the reasons why our 60-year-old personnel clearance system is not only inefficient but ineffective in providing the United States with the security it needs. Our risk avoidance culture is based on threats, societies,

and a pace that is well in our past. Not only do we not take advantage of technology, we are hindered by it. We attempt to avoid risk in a desire to achieve unachievable goals of absolute security, and in the process we are now creating vulnerabilities for others to capitalize on. Today, companies around the world have understand that risk cannot be avoided, but must be managed. It is past time for our government to adopt the same philosophy.

We propose moving from a "risk avoidance" security culture to one based on "risk management." In a risk management culture, the system acknowledges the element of risk at the beginning of the process, but instead has mechanisms that would allow that risk to be mitigated because of a robust ability to detect issues on a day-to-day basis. Examples of such a culture can be found in the financial marketplace where companies generally "clear" their employees – who arguably handle extremely sensitive financial information that can equate in sensitivity to much of our "classified" national security secrets – within two weeks. Afterward, however, there is a process of continuous evaluation and compliance that ensures adherence to the stringent guidelines warranted by the sensitivity of the data. The financial sector's ability to "clear" individuals so quickly is based on a fully automated system of extensive record and data base checks that, in today's world can present a detailed understanding of someone's life; such a detailed picture would be as revealing as information derived from a field investigation, if not more so, and in a small fraction of the time. This initial clearance is followed up by a continuous monitoring and evaluation process that mitigates further risk.

An example of the "continuous evaluation" process (as well as reciprocity) can again be found in the financial sector, this time in the credit card area. If I were in Sydney, Australia today, I could take my Visa Card and put it into an ATM machine. The machine would read the date on the card, compare it with a data base of financial records and, having established the legitimacy of the card would respond and "say" "G'day, Tim." I could then take out significant amounts of money and walk away. In this scenario, the banking industry has taken on an element of risk. First, that I have money in the account or an available credit balance, which is quickly ascertained by data base checks before the money is given. A second element of risk is whether or not the legitimate card holder is presenting this card. To mitigate that risk, there is a continuous evaluation aspect that runs silently in the background and monitors my account/card usage. Should something out of the ordinary – as defined by my normal spending habits that have been monitored – transpires, action is taken, usually by a telephone call to me asking about recent purchases in order to either confirm that everything is alright or to identify a breech in security of the system. In most cases, such credit card or identity theft is quickly identified and acted upon. An example of reciprocity in the system is that I can walk up to any ATM machine in Sydney, or anywhere else in the world, regardless of whether it is "my" bank and have the same result.

Mr. Chairman, there is no reason that the government could not adopt similar processes for granting security clearances as those I've just described and virtually wipe out backlogs as well as increase our overall security. Such a system could allow the government to immediately determine suitability and grant or decline a clearance to the

majority of applicants, and employ traditional field investigations when necessary. Although the level of clearance required for an individual's initial application would be based on a specific job, once obtained the clearance would be assigned to the individual for his lifetime and would be continuously monitored and adjusted based on a continuing assessment and evaluation process. The elements of such a system would include:

- A fully automated, government-wide application systems, including electronic fingerprinting.
- A centralized, automated investigation that would perform significantly robust database checks on applicants in order to create a "score" assessing a level of risk, much like your credit score. Such database checks would far exceed today's National Agency Check with Law and Credit (NACLC), currently required for SECRET and TOP SECRET clearances, and be more robust than current data collected from most field investigations.
- An automated adjudication system that would take an applicant's score and compare it with the acceptable level of vulnerability for the specific job for which the individual applied. Should the scores compare favorably, a clearance would be granted. For those that do not compare favorably, the system would generate a human adjudication process, which could also lead to a field investigation.
- An automated, continuous evaluation system that would run in the background and would adjust an individual's score on a near-real time basis. Such an evaluation would detect significant changes or deviations that would trigger an investigation, depending upon the risk and vulnerability assessments of the job.
- A system of aperiodic investigations. Such investigations may be completely random, based on the vulnerability or sensitivity of a specific position, or may be triggered by detection of an anomaly through the continuous evaluation process.
- A robust, government-wide counterintelligence process that would compliment this new system by assessing the threat environment and monitoring developments that would be linked to certain jobs, facilities, and programs.
- All systems would be based primarily on newly purchased commercial-off-the-shelf (COTS) technology, phasing out existing legacy systems as rapidly as possible
- The overall process would be governed by a new set of government-wide laws, regulations, Executive Orders, and standards.

Such a system would reallocate human resources. Although there would be some human investigations and adjudication associated with the initial investigations, the bulk of these resources would be shifted to incident and aperiodic reinvestigations, thus increasing security in areas where we are most vulnerable today.

Mr. Chairman, let me stress that this is not a cost savings plan, at least in the near term. Security cannot be accomplished "on the cheap." Resource "savings" from limiting the number of initial field investigations, would be allocated to those areas where we can best mitigate risk through aperiodic reinvestigations. That said I believe that over time the government would save considerable expense in terms of opportunity costs associated with working for the government. Nor would implementation be simple. I do believe, however, that it is obtainable. Finally, I must emphasize the need to incentivize security officers to adopt such a dramatic cultural change.

Creating such a system will require resolve, especially at the senior levels of the Executive and Legislative Branches. Heretofore, government leaders have relegated security to an administrative function. Only recently have they begun to fully understand the significant impact of the processes itself as well as the bureaucracy that supports it. For the first time, senior leaders in the Department of Defense, the Intelligence Community, the White House, and other departments of government have are coming to an understanding that there must be significant and dramatic changes to the personnel security clearance process. These efforts will be enhanced by Congress' continued focus. I appreciate this development and believe that now is the time for dramatic transformation.

Conclusion and the Need to Act Now

Mr. Chairman, it has been just over one year since the Defense Security Service (DSS) announced that they were suspending the acceptance and processing of industry clearances because they were out of funding. Since that time, I can find no improvements to the overall government clearance process that would prevent a recurrence of such a suspension within the next six months, despite efforts by the current DSS leadership. As the Department of Defense comprises the bulk of requirements (in terms of numbers) for individuals with security clearances, the DSS dilemma is a stark indicator that the government's current personnel security process cannot meet today's needs. Certainly, a portion of the problem is that today's system is very labor-intensive and is completely out of step with today's demands in a highly information technology rich world. More importantly, the fundamental premise of today's process must change to better address today's society, the information environment within which this society exists, and the needs that the government, especially the Intelligence Community, has for engaging our society's rich cultural mix in order to have the best and brightest as part of the effort to protect our nation. Most importantly, today's process does not adequately meet today's threats, let alone those in the future. Therefore I implore the Committee to consider the larger picture and support the significant but necessary changes I have offered. Thank you.