



AN INSA WHITE PAPER PREPARED BY  
THE INSA COUNCIL ON SECURITY AND COUNTERINTELLIGENCE

*October, 2007*

## **IMPROVING SECURITY WHILE MANAGING RISK**

*How Our Personnel Security System Can Work Better, Faster,  
and More Efficiently*

# CONTENTS

<b>Preface</b> .....	1
<b>Executive Summary</b> .....	3
<b>Statement on Scope and Purpose</b> .....	4
<b>Introduction: Where We Are and How We Got Here</b> .....	5
<b>Part I: Expectations of a Personnel Security System</b> .....	7
Keeping the Wrong People Out.....	7
Getting the Right People In.....	7
Filling National Security Positions in a Timely Manner.....	8
Detecting Security Threats within the System.....	9
Using Resources Efficiently.....	10
<b>Part II: Recommendations for a Better, Faster, and More Efficient Personnel Security Clearance System</b> .....	13
Recommendation 1: Utilize a Comprehensive Database Search as the Baseline for All Security Clearances.....	13
Recommendation 2: Institute a Comprehensive, End-to-End, Electronic Case Management System.....	14
Recommendation 3: Integrate a Robust Counterintelligence Program.....	14
Recommendation 4: Enhance and Enforce Laws and Policies Mandating Uniform Clearance Standards and Reciprocity of Clearances.....	15
Recommendation 5: Create a Government-wide Central Repository of Security Clearance Status Information All Cleared Individuals.....	15
Recommendation 6: Conduct a Comprehensive Review of Previous Studies on Anomalous Behavior for Indicators of Insider Threat.....	15
How These Recommendations Will Improve Personnel Security.....	16
<b>Conclusion</b> .....	19
<b>Appendix A: Current Process Basics</b> .....	21
<b>Appendix B: Current System vs. New System Flow Charts</b> .....	23
<b>Appendix C: Hypothetical Cases under the New System</b> .....	25
<b>Appendix D: About the Intelligence and National Security Alliance</b> .....	27

# PREFACE

## **The Intelligence and National Security**

Alliance (INSA) and its Committee on Security and Counterintelligence are pleased to present this white paper on transforming the government's personnel security process. The government's security clearance process has both direct and indirect effects on almost every aspect of national security operations, yet, until recently, its importance has rarely been acknowledged. In most cases, government leaders have relegated security to an administrative function. Recently, some government leaders have begun to fully understand the significant impact of the security processes themselves as well as the bureaucracy that supports them. For the first time, senior leaders in the Department of Defense (DoD), the Intelligence Community (IC), the White House, and other departments of government have all come to an agreement that there must be significant and dramatic changes to the personnel security process. INSA applauds this initiative and supports efforts to affect meaningful change.

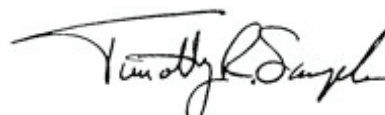
One of the first major initiatives to reform the clearance process was with Secretary of Defense Casper Weinberger's Security Review Commission in 1985. More recently, the Intelligence Reform and Terrorism Prevention Act of 2004 called for changes in the situation surrounding the backlog of hundreds of thousands of individuals awaiting clearances by calling for a more consolidated approach and legislating timelines for clearance process completion. Despite such efforts there has been no appreciable difference in the situation; certainly not at a government-wide scale. Today's processes are flawed and cannot meet government requirements nor address the future threat environment. We appreciate the ongoing efforts by a DSSC special team, comprised of individuals from Office of the Director of National Intelligence (ODNI) and the Under Secretary of Defense (Intelligence) (USD(I)), looking

into this issue. The preliminary reports indicate that their collective efforts are coming to conclusions similar to those presented in this paper. We hope that our report, as an independent, unbiased view, helps their efforts.

INSA remains a member of the Information Technology Association of America (ITAA) coalition of associations that has been speaking out over the past few years on the need to transform the current system by introducing automation and standardization to the process in order to erase the significant backlog of security clearance cases. However, a major transformation — in philosophy and culture — is needed in order to adequately protect our nation's security. This white paper presents the case for such a transformation and provides recommendations that the government should consider in order to create a personnel security clearance process that is fitting of today's and tomorrow's security environment. The views contained in this paper do not necessarily reflect the views of all individual and corporate INSA members.

We hope you find this paper enlightening. Today, we have the potential to create a personnel security system that operates efficiently and truly meets our needs. We welcome your comments and suggestions, just as we welcome the opportunity to continue to support efforts to improve our personnel security system and processes.

Sincerely,



*President*  
Intelligence and National Security Alliance



# EXECUTIVE SUMMARY

Background investigations for those in national security positions are critical to ensuring that our nation's most valued information is protected by loyal, honest, trustworthy individuals. The system and standards the United States government uses to determine a person's eligibility for a security clearance have remained roughly the same since the 1940s, when the use of security clearances (either as producers of classified information or as consumers) numbered in the hundreds. A combination of societal and technological changes, along with the exponential growth in the volume of classified information and in the size of the workforce — in and out of government — that requires security clearances indicate the need for changes to a system that is both outdated and overloaded.

An ideal security clearance process should accomplish five main objectives: first, it should keep the wrong people out of critical national security positions. Second, it should get individuals with the skills our nation needs into those positions. Third, the system should fill all national security positions in a timely manner so that critical work can be completed. Fourth, the ideal system should promptly detect insider threats and minimize their damage to our nation's security. Finally, the system should use its resources effectively and efficiently.

The current system does a fair job of meeting this first objective: keeping the wrong people out. However, the current system is weighted toward that objective above all else, resulting in many of its most obvious and critical flaws. For example:

- First- and second-generation Americans with critical language skills and cultural understanding are frequently labeled security risks because of their family ties or travel overseas;
- Today's process of investigating individuals utilizes outdated or no technology and takes an exorbitant amount of time;
- The criteria used to evaluate candidates are essentially the same criteria used when the system was established in the late 1940s, and it is unclear if those criteria are still relevant today;
- Qualified applicants' desire to serve the nation is frequently overcome because of the excessive time it takes to obtain a clearance. Instead, they forgo national service in exchange for immediate, meaningful employment;
- Security clearance delays and backlogs have turned cleared personnel into a marketable commodity, ultimately driving up the cost of government contracts;
- Interagency reciprocity of clearances remains the exception rather than the rule, causing a lengthy and cumbersome process for individuals transferring between two cleared positions.
- The current system falls short of effectively and efficiently detecting insider threats. Reinvestigations are only scheduled every five years, and as a result, the potential for damage to our national security during those five years is great. Moreover, it is unclear whether the current system can identify "new" indicators of insider threat (e.g. Web postings) along with

more “traditional” indicators (e.g. travel and group affiliation).

INSA proposes six recommendations to address these issues:

- **Utilize a Comprehensive Database Search as the Baseline for all Security Clearances.** There are hundreds of commercially-available databases capable of collecting information on nearly every aspect of a person’s life, potentially as robust as uncovered in a field investigation but at a fraction of the cost and time.
- **Institute a Comprehensive, End-to-End, Electronic Case Management System.** This will automate and expedite the clearance process as well as better manage investigative resources.
- **Integrate a Robust Counterintelligence Program.** Convicted spies Robert Hanssen and Aldrich Ames operated within the system for decades, at the cost of many lives and millions, if not billions, of dollars. A robust counterintelligence program is critical to protecting national security secrets.
- **Enhance and Enforce Laws and Policies Mandating Uniform Clearance Standards and Reciprocity of Clearances.** Despite more than fifty years of legislation and executive orders establishing uniform criteria for baseline investigations and adjudication standards, there

is still a lack of consistent, government-wide standards for each level of clearance.

- **Create a Government-wide Central Repository of Security Clearance Status Information for All Cleared Individuals.** Such a system would greatly improve reciprocity and would tie an individual’s clearance to his person and not his position, reducing delays when changing jobs.
- **Conduct a Comprehensive Review of Previous Studies on Anomalous Behavior for Indicators of Insider Threat.** A complete understanding of motivations and indicators of insider threats is essential in targeting and mitigating them.

By implementing the recommendations in the paper, INSA believes the government can dramatically improve our national security structure. These recommendations will not only improve the quality and efficiency of the system, but also make the system more secure while mitigating risk. INSA remains ready to assist the government in implementing these needed changes.

## Statement on Scope and Purpose

This paper does not delve into “the weeds” of personnel security, a process that employs tens of thousands of personnel, numerous agencies and departments, and billions of dollars. No two agencies or departments within the

government have the same system for issuing a clearance, despite the fact that they are all striving to meet the same established, government-wide criteria. Some agencies have processes that work more efficiently than others, but all agencies are hampered by outdated technology and perspective. None have security processes that readily adapt to a changing, more transient workforce. Therefore, this paper focuses not on the details of each agency or department’s processes, but on the basic goals and functions of what a personnel security system should be in order to best protect the nation. This paper focuses on improving upon the functions of the system, but does not outline any particular form for achieving those aims. There are a variety of structural options that the government can pursue with success as long as the new system meets its main objectives.

The appendices provide a brief overview of the current system and how a new system could work more efficiently. Best practices from the private sector are discussed generally; however, specific commercial systems are not identified as part of the recommendations for security, proprietary, and other reasons.

# INTRODUCTION

**The National Security Act of 1947 delegated the authority and responsibility of granting access to classified information to the Executive Branch. When created, the program was appropriate to accommodate the size of government and the amount of classified information that needed to be protected. The system relied on an extensive, front-end evaluation of a candidate's eligibility for access to classified information and a periodic reinvestigation, usually every five years. As the government grew, so did the security bureaucracy in order to address the growing number of individuals requiring clearances. The system flourished and, arguably, adequately protected our nation's secrets, albeit with some notable, extremely damaging exceptions.**

Despite significant changes in technology and to the national security workforce, today the government uses essentially the same system first implemented sixty years ago. The system has not embraced technological advances, such as the ability to verify personal information in private and commercial databases. In addition, outdated techniques, such as the field investigation, are based on a society very different from the one today. Consequently, questions like, "does the applicant live within his means?" had much more relevance in 1947 than in 2007, especially in terms of the interviewee's ability to answer this highly subjective question. Furthermore, today's workforce is highly mobile, but the system continues to operate under the assumption that a cleared employee would serve her entire career within the government and probably within the same agency. Today's workforce must be able to refresh its skills and its composition more rapidly than in the past. Put simply, today's

system is designed to address a workforce that no longer exists.

In the mid and late 1990s Congress started to rebuild the nation's intelligence, defense, and security capabilities that had been decimated as part of the "Peace Dividend" following the Cold War. By the late 1990s the system was coping with the first security clearance "backlogs," a result of personnel increases during this period. The September 11, 2001 terrorist attacks, and the rapid hiring thereafter, greatly exacerbated the clearance problem both for government agencies and industry, which took on more classified work to meet the government's needs. Although there have been some recent improvements in reducing the time it takes to get a clearance, it frequently takes a year or more for an individual to receive an initial clearance or for completion of a re-investigation. Table 1 provides a view of the current situation.

**TABLE 1: Average Time Required to Grant Eligibility (in days)**

	Application Verification	Investigation	Adjudication	Total
Initial Clearance	111	286	39	446
Reinvestigation	81	419	36	545
IRTPA Requirement for 80% of all cases	14	90	30	120 (134)

Source: GAO Study on DoD cases adjudicated in January and February 2006. Note that IRTPA does not calculate the number of days it takes to verify that the application is complete in its total 120-day requirement.



# EXPECTATIONS OF A PERSONNEL SECURITY SYSTEM

The problems associated with the current system have been detailed many times in many different ways. This paper doesn't, therefore, spend time re-examining each of those problems. Instead, it offers a new perspective for evaluating the success of any personnel security program. We've established five basic requirements critical for a successful system: keeping the wrong people out; getting the right people in; filling national security positions in a timely manner; detecting security threats within the system; and using resources effectively and efficiently. Then we evaluate the current system in its ability to meet these expectations. As detailed below, our current personnel security system is failing to meet some of these basic requirements.

## Keeping the Wrong People Out

**The most basic element of a security system** is to ensure that it is not being penetrated by someone intent on doing harm. From the founding of a government-wide security system, the original intent was to ensure that those persons privileged to hold positions in national security with the government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.

On the whole, our current system has been adequate at keeping out individuals who are not suitable for access to classified information. Spies are generally thought to be an aberration in the federal government. There have been very few "penetrations" of our security system; that is, individuals who enter into national security service with the specific intent of gathering information to pass to a foreign government. One notable exception was Ana Montes, who entered the national security system with the intent of spying for Cuba. Reportedly, from 1980–2000,

the Pentagon reviewed eighty espionage cases and found only two individuals who penetrated the security system in this manner.

The far more serious threat to national security secrets comes from those who enter the system with good intentions but choose during the course of their career to betray the country. The recent and most damaging espionage cases have involved this "insider threat." Aldrich Ames and Robert Hanssen are examples of individuals who were considered to be good and trustworthy when they first entered service, but succumbed to disillusionment, family problems, or other personal stresses and eventually betrayed the United States.

## Getting the Right People In

**Beyond keeping the wrong people out of** national security positions, our personnel security system has to be able to get the right people in positions where they are critically needed. In short, this means that the government needs to get individuals with certain scientific, academic, and

analytical skills into the national security system where they will be most effective. Particularly after 9/11, the country needs individuals with specific language skills and cultural understanding in order to fight terrorism and other critical national security threats.

As senior intelligence community leadership has noted, it is very difficult to get first- and second-generation Americans into critical national security positions under the current system. Today's system does its best to eliminate risk by denying clearances to individuals who have spent time in or have family residing in certain foreign countries. For the system, this eliminates risk of coercion or blackmail of an individual through those foreign family ties. Unfortunately, these are the Americans who have the language skills and cultural understanding the government desperately needs.

## Filling National Security Positions in a Timely Manner

**Another imperative of a** personnel security system is filling critical national security positions in a timely manner. Although timelines vary from agency to agency, it can take a year or more for an individual hired to a national security position to receive his clearance. The damage this causes is self-evident: for example, the national security community clearly suffers from a lengthy clearance

delay in bringing on an Iranian nuclear proliferation expert.

Filling national security positions in a timely manner presents the most difficult challenge to the current system and is the issue that has gained the most notoriety with Congress and the American public. Although some Intelligence Community agencies have addressed this issue and can employ individuals significantly faster than other agencies, such efforts are restricted to a relatively small number and are often the exception rather than the rule. The reasons for such delays are well known:

- A heavy reliance on initial full-field investigations;
- Insufficient resources for logistical and administrative support to field investigations;
- A labor-intensive and slow investigative and adjudicative process;
- The lack of an automated case management system;
- A lack, in some agencies, of trained, experienced adjudicators;
- An inefficient and disruptive relationship between government agencies.

It is important to note that the government hiring boom following 9/11 is not the cause of the current security clearance backlog. A study released by the Defense Department's inspector general in February of 2000 calculated that there were more

than 900,000 people awaiting Pentagon security clearances, only 400,000 of which had even been started. Furthermore, DSS had yet to open over 500,000 cases of people due for reinvestigation. At that time, it took DSS an average of 306 days to grant an initial clearance, and 300 days to complete a reinvestigation. DSS no longer is responsible for

## FILLING NATIONAL SECURITY POSITIONS IN A TIMELY MANNER PRESENTS THE MOST DIFFICULT CHALLENGE TO THE CURRENT SYSTEM AND IS THE ISSUE THAT HAS GAINED THE MOST NOTORIETY WITH CONGRESS AND THE AMERICAN PUBLIC.

security clearance investigations — having been directed to give investigations to the Office of Personnel Management in a fee-for-service contract. As previously noted in Table 1, however, the timelines under this arrangement remain substantial. The post-9/11 hiring boom exacerbated and highlighted the existing deficiencies. The importance of this issue will continue to increase as our national security responsibilities and requirements for cleared personnel expand to include homeland security.

## Detecting Security Threats within the System

**Counterintelligence (CI)** is often an overlooked but crucial component of the national

security system, including in support of an effective personnel security process. The ability to detect and identify threats of penetration or disruption in a timely manner is critical. CI capability is the difference between effectively protecting secrets and allowing severe, if not grave, damage to our national security.

Today's system does not have adequate security and CI capabilities to detect insider threats until significant damage is done. Although there are periodic reinvestigations of cleared personnel, they are based on a predictable schedule of five years for TOP SECRET clearances and ten years for SECRET clearances. Consequently, it is possible to

"game" the current system, with catastrophic results. A good foreign intelligence service can target a cleared worker immediately after his investigation with the knowledge that it will have at least four and a half years to exploit his access. Furthermore, because the individual knows when his re-investigation will be, he has the opportunity to rehabilitate his

## UNINTENDED CONSEQUENCES: THE MARKET FOR CLEARED PERSONNEL

As a result of lengthy clearance delays, a security clearance is now highly "marketable." As mentioned before, the need for workers with clearances has increased dramatically in both the government and private sector. Combined with the significant time required to get an initial clearance, this has led to a significant demand to hire individuals who are already cleared, particularly within the private sector.

The result is an inflated job market for cleared personnel. In some cases, this can mean significant bonuses and a salary structure of up to 35 percent higher than someone without a clearance. A report published by *Washington Technology* in July of 2007 stated that the gap between salaries for people in the same positions can be nearly \$40,000 based solely on the possession of a clearance. Consequently, the competition to entice an individual from one company to another, or from the government to the private sector, 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.

Another factor contributing to this market is an acquisition process for classified contracts usually requiring companies to "bid" only individuals already possessing a clearance. Bidding only cleared personnel often means bidding individuals currently on other classified contracts, with the hope of being able to replace them with new individuals as their clearances are finally granted. One serious byproduct of this cycle is that the government misses out on new perspectives or ideas because the same cleared people are being used on projects again and again. If a company hires an individual and is able to submit for an initial clearance, the company may have to keep the employee on the books for more than a year giving her "busy work" if there are no unclassified contracts available to utilize her talents. Legitimately, a company must factor these individuals into its overhead costs which ultimately get charged back to the government, resulting in more cost to the government per contract. Sometimes an individual may leave the company before the contract award because they have found more immediate and meaningful work with another company.

lifestyle before the reinvestigation begins. Aldrich Ames and Robert Hanssen spied for years and passed reinvestigations before they were finally caught only after they caused irrevocable damage to national security programs.

Beyond reinvestigation timelines, there are other problems with current procedures. First, employees are expected to report suspicious activity to their managers, who are often reluctant to report that activity for fear of disrupting the working environment or of retribution or litigation should the concerns be unwarranted. Second, today technology has developed to the point where every keystroke of an employee can be monitored, but even basic measures for collecting, processing, and analyzing this type of data have yet to be implemented. Most importantly, U.S. CI programs have been historically under-funded and under-prioritized. Moreover, CI and security have often run in parallel tracks of activity and responsibility when they need to run as a collective, collaborative, and complementary process.

## Using Resources Effectively and Efficiently

### As with any government

process or program, there is an expectation that the personnel security system should operate efficiently; that is, not needlessly expend resources. In a personnel

security clearance process, this means that the system should incorporate cost-saving technology wherever possible; design compartmentalization and clearance processes that are appropriate to the work; minimize the impact of an employee transferring between two cleared positions; and investigate and adjudicate only on the criteria that truly determines whether or not someone should have access to classified information.

In respect to technology, the current system falls drastically short of meeting any efficiency standard. Despite technological advances, the current system relies heavily on people and paper to assemble, scope, dispatch, and investigate cases. Utilization of commercial overnight couriers is a common delivery method for case-file traffic among and within agencies. Though a computer could accomplish the same task more efficiently, people are the primary form of case management. Despite the existence of databases that can collect much of the data more quickly, full field investigations are the baseline for investigation of all TOP SECRET clearance requests. The Office of Personnel Management (OPM) has declared that it will soon have all new case files “imaged,” meaning scanned or photographed into a virtual file. Imaging documents is short-sighted; all files should be fully editable, online, and capable of being sent

and updated electronically; not just an electronic version of a hard copy document.

Among the many complaints lodged against the current personnel security clearance system, few draw as much ire as its lack of

## GONE ARE THE DAYS WHEN MOST MEMBERS OF THE WORKFORCE STAYED WITH A PARTICULAR AGENCY FOR THEIR ENTIRE CAREER.

reciprocity. Despite federal law establishing uniform, government-wide standards for clearance investigations, various agencies and departments frequently add their own exceptions and investigational standards. This goes much beyond some agencies requiring polygraphs. These different investigative standards enable various agencies to refuse other agencies’ clearances, making Congressionally-mandated reciprocity problematic. In addition, this has forced OPM to conduct a staggering number of different types of TOP SECRET investigations in order to meet the specific agency requirements. Furthermore, there is not even a single system for verifying the status of an individual’s clearance. JPAS, Scattered Castles, DCII, and OPM’s Clearance Verification System are some of the main systems that hold clearance data, but these systems are not interconnected, and an alarming number of clearances have to be confirmed

through phone or fax on a daily basis. Gone are the days when most members of the workforce stayed with a particular agency for their entire career. Today people change jobs frequently, which create detrimental delays as they wait for their clearance to be accepted by a new agency or for a new investigation at the same level because the previous investigation was deemed insufficient for the new job.

Another major inefficiency in the current system is that the clearance level required for many positions is inappropriate to the amount of risk that work entails. The person drilling the rivets on an aircraft may well have the same clearance as the person designing the weapons system on that plane. The investigation of the mechanic receives the same time, money, and scrutiny as the investigation of the engineer, even though the two pose a very unequal security risk.

It is unclear if the criteria used to grant a clearance, and the means to collect applicant data, are still appropriate. Thirteen of the fourteen “decision points” currently used to evaluate if a candidate is eligible for a security clearance are vestiges of the system created in the 1940s. Since then, society, our ways of communicating, and perhaps even the reasons why individuals spy have changed. In the ‘40s and ‘50s, neighborhoods were tightly interwoven communities. Not only

did people know their neighbors’ names, but they knew intimate details about their neighbors’ lives and attitudes. A neighborhood field investigation was a logical way to collect information about someone’s personal life. Today the opposite is more likely to be true. A larger proportion of Americans live in major metropolitan areas than ever before, and people are less likely to know personal information about their neighbors. It is imperative that the questions asked in application paperwork, personal interviews, and during field investigations solicit quality information that truly determines whether a person is worthy of access to classified information. When a field investigator asks, “Does the applicant drink a lot?” the interviewee will likely answer the question within their personal frame of reference, possibly resulting in dramatically different accounts of the same person’s behavior. Another highly subjective question is if the applicant “lives within her means.” Most neighbors, co-workers, and references do not know the applicant well enough to answer that question with confidence.



# RECOMMENDATIONS FOR A BETTER, FASTER, AND MORE EFFICIENT PERSONNEL SECURITY CLEARANCE SYSTEM

Previous attempts at personnel security clearance reform have tried to address some of the issues laid out in the previous section, but true reform must be transformational. Personnel security can never be perfect in stopping spies and others intent on harming national security, but it can catch them early and minimize the damage they cause. Below, six recommendations are outlined for dramatically improving the way personnel security works in this country. While not perfect, the incorporation of these recommendations will substantially enhance the way personnel security works, ensuring that the country is able to accomplish the national security work it needs while minimizing the damage of those intent on harm. This new system should have the following aspects:

- Accepting, but minimizing risk during the initial investigative phase, while creating a deterrent to insider threat through a system of continuous monitoring and aperiodic reinvestigations;
- Taking advantage of electronic databases that currently exist and have a robust level of information on almost every individual;
- Incorporating the latest technology in the process in order to increase efficiency, enhance management, and create better accountability;
- Improving reciprocity through a standardized process across the government while still allowing a federated process in some circumstances in order to address key, limited additional factors;
- Strengthening reinvestigation and counterintelligence processes; and
- Creating a process that focuses on each individual throughout their lifetime and attaches the clearance to their person and not their position.

## **Recommendation 1: Utilize a Comprehensive Database Search as the Baseline for All Security Clearances**

**In recent years, electronic databases have** proven to be reliable and robust methods of collecting information on individuals, though the government has yet to incorporate them into the clearance process. Utilizing a comprehensive, automated database search will leverage advances

in technology while dramatically improving efficiency in the system. Databases have access to an extensive array of public and private data and are able to collect on virtually all of the decision points needed for a clearance. Such databases are available today, and can be combined with standard national security, criminal/law enforcement, and financial checks currently used to gain an accurate picture of a candidate's life.

One major benefit of using electronic databases is that they can continuously monitor an individual's lifestyle, much like a credit score. The government should establish an automated "scoring" process to continuously evaluate a person's security risk. For example, purchasing a house with cash, a series of DWI convictions, or frequent solitary travel abroad are types of suspicious behavior that a continuously updating system could monitor and flag for reinvestigation. If these are isolated incidents, the person should be cleared and experience no disruption in work. If there is not a reasonable explanation for the suspicious behavior, the system was successful in quickly identifying security risks that under the current system might have gone unnoticed for years. This "security score" will be weighed against a range of acceptable scores

for each position, as established by the office where the position resides. This score should be used for initial requests and for continuous monitoring, highlighting serious anomalies and, where appropriate, triggering an aperiodic re-investigation. The "security-score" would remain with the individual throughout his career. (See Appendix C for an example of how such a process would work.)

### **Recommendation 2: Institute a Comprehensive, End-to-End, Electronic Case Management System**

**It is past time for the** creation and implementation of a government-wide case management system that completely automates the investigative process in the field and at the central facility. This will allow for immediate, electronic transfer of case files among investigative and adjudicative components, eliminating the current paper-driven process. Moreover, the system allows managers to monitor the progress of each case in the system in order to better understand and manage workload in the field and to better identify and control cases where incomplete information may cause delays. There should be one case management system for the government, with multiple access levels for management and

for levels of security clearance information. An end-to-end case management system should also be transparent, allowing security officers across the government and private sector the ability to obtain the status of clearance requests.

### **Recommendation 3: Integrate a Robust Counterintelligence Program**

**Counterintelligence is the** last and most important line of defense when protecting national secrets. Nevertheless, CI is often dramatically under funded. Strengthening counterintelligence capabilities must be part of security clearance reform. Under the recommendations proposed here, a more robust monitoring and CI process should have the ability to monitor an individual through continuous evaluation of a person's "security score" in database checks; reinvestigate on an aperiodic basis; and look for indications of espionage, sabotage, questionable behavior, and other insider threats.\*

It is important to note that in the latest definition of CI from the National Counterintelligence Executive NCIX, personnel security programs are specifically *not* included. Although we commend the current emphasis on CI and progress that NCIX is making, it is important to note that the insider

---

\* The focus of this paper is personnel security. INSA notes, nevertheless, its concern that security and counterintelligence remain significantly under funded and underestimated in American intelligence. Too often, these critical functions have been relegated to low-level (and unattractive, in career terms) administrative functions, when they should operate as highest-level strategic priorities. The Intelligence Community should consider a major research effort into designing security and counterintelligence capabilities for the 21st century information environment.



threat issue demands a very close relationship and interaction between personnel security and CI programs.

#### **Recommendation 4: Create a Government-wide Central Repository of Security Clearance Status Information for Every Person Holding a Clearance**

**Although a federated system** of investigation and adjudication to meet some unique agency issues is important, centralization of information pertaining to clearance status is essential to improving reciprocity. Such a system will also emphasize that clearances are associated with the individual, not the position he holds. This will require significant measures to protect data and privacy issues, but the benefit of a single, central repository of clearance information cannot be overstated. This centralized repository will also facilitate continuous evaluation of cleared individuals. Obviously such a repository needs to be highly secure and constantly monitored against unauthorized access.

#### **Recommendation 5: Enhance and Enforce Laws and Policies Mandating Uniform Clearance Standards and Reciprocity of Clearances**

**Another key component** of a new system is the creation of standardized criteria for training, investigating and adjudicating in order to establish a single,

government-wide process for baseline clearances that would be common for all parts of the government. Despite sixty years of legislation and executive orders establishing uniform criteria for investigation and adjudication standards, there is still a lack of consistent, government-wide standards for each level of classification. Although there are clearly additional components required for some agencies and offices dealing with our most sensitive information, the majority of additional investigative

#### **WITH A STANDARDIZED BASELINE, THE GOVERNMENT WILL HAVE BETTER QUALITY CONTROL OVER THE INVESTIGATION AND ADJUDICATION PROCESS.**

standards placed on clearances today are not needed. With a standardized baseline, the government will have better quality control over the investigation and adjudication process. It is also past time for a standard, government-wide application process, including acceptance of electronic and biometric identifiers such as fingerprints.

Due to the importance of implementing a new system as envisioned in this paper, INSA suggests that the government consider a complete new set of laws, regulations, policies, and executive orders, superseding all existing guidance and establishing

the government-wide baseline that is needed. Such a move should clarify for security officers and others the intent and importance of this new security clearance process.

#### **Recommendation 6: Conduct a Comprehensive Review of Previous Studies on Anomalous Behavior for Indicators of Insider Threat**

**We have to know what to look** for in order to stop and deter the insider threat. Inherent in any counterintelligence program or reinvestigation process is an identified need to be able to determine behaviors, or indicators of behaviors, that may be associated with illicit activities. In essence, this means that base-lined 'normal' behavior must be characterized so that anomalous behaviors can be alarmed in an automated system. To our knowledge, there has never been a comprehensive study of normal or anomalous behavior to determine what the warning signs are when someone has started to spy. Thirteen of the fourteen decision points currently used to evaluate if a candidate is eligible for a security clearance are a vestige of the system created in the 1940s. Since then society, our ways of communicating, and perhaps even the reasons why individuals spy have changed.

This leads to perhaps the most important question: when clearing or reinvestigating individuals, are we asking the right questions? How

important is it that someone's credit score has gone up? That his travel abroad has increased? That he has developed a drinking problem? That he is posting to certain Web sites? Armed with better information on what to look for, managers, counter intelligence officers, and fellow co-workers can identify suspicious behavior faster, minimizing the impact of the insider threat.

#### **ARMED WITH BETTER INFORMATION ON WHAT TO LOOK FOR, MANAGERS, COUNTER INTELLIGENCE OFFICERS, AND FELLOW CO-WORKERS CAN IDENTIFY SUSPICIOUS BEHAVIOR FASTER, MINIMIZING THE IMPACT OF THE INSIDER THREAT.**

It is imperative that the government conduct basic research to identify the normal behaviors as well as anomalous behaviors that would be used as indicators for reinvestigations and counterintelligence activities. Normal and abnormal behavior can be grouped by many factors, such as position, level of access, and duties. This study, coupled with the continuous evaluation process, would be able to quickly identify anomalous behaviors and minimize the damage caused by the insider threat.

#### **How These Recommendations Will Improve Personnel Security**

Implementing these recommendations will make major improvements in protecting national

security, but structural changes alone are only half the battle. Along with structural and technological change, a cultural shift must also occur. This includes:

- Placing emphasis on getting qualified people to work as quickly as possible;
- Changing the incentives for security officers to place more focus on catching spies and insider threats rather than placing overwhelming emphasis on the initial clearance process;
- Developing a robust counter-intelligence model that allows better capability in identifying threats early rather than simply reacting to them;
- Mitigating and managing risk, rather than attempting to avoid risk altogether, by trusting an automated system, without a full field investigation, especially for SECRET/collateral clearances; and,
- A willingness to adopt a single, government-wide system for security clearance investigations, given that some of the system may be federated due to certain agency restrictions.

With these recommendations, a comprehensive security clearance process will develop, which will dramatically reduce time and costs for obtaining a clearance while increasing our overall security. Consider how this system better meets the criteria we used to evaluate the current system in

Part 1:

#### ***Keeping the Wrong People Out***

This system will continue to identify those who are not suited for access to classified information, but do so in a timelier and less costly manner. For those who require SECRET/Collateral clearance, this process should take no more than two weeks.

#### ***Getting the Right People In:***

Under this new system, those who qualify for access to classified information should be able to start sooner than under the current system. With continuous monitoring and robust CI, the risk presented by first and second-generation Americans is mitigated far better than under the current system.

#### ***Filling Critical National Security Positions in a Timely Manner:***

These structural and technological recommendations will dramatically reduce timelines for completion of clearances, allowing critically needed skilled workers to start work in a timely manner. Furthermore, these recommendations take a great step toward eliminating the competition for cleared personnel. Significantly reducing the time required to receive a clearance begins to eliminate such competition, ultimately saving industry and government significant amounts of money.

#### ***Detecting Security Threats within the System:***

With continuous monitoring, aperiodic investigations, and more

robust CI, the new system will not only detect insider threats faster, but will create a credible deterrent against those seeking to harm the national security structure.

***Using Resources Effectively and Efficiently:***

Under today's system, there will never be enough field investigators or adjudicators, even with outsourcing, to keep up with growing security requirements. A new system that heavily invests in technology, knits together the clearance process through the national security community, and uses human resources only when necessary will significantly improve efficiency. In addition, reciprocity will improve by using a standard system for the baseline clearance process, even considering

**A NEW SYSTEM THAT HEAVILY INVESTS IN TECHNOLOGY, KNOTS TOGETHER THE CLEARANCE PROCESS THROUGH THE NATIONAL SECURITY COMMUNITY, AND USES HUMAN RESOURCES ONLY WHEN NECESSARY WILL SIGNIFICANTLY IMPROVE EFFICIENCY.**

that some agencies may have additional security requirements. The continuous monitoring on individuals holding clearances will translate into a greater ability to minimize damage, encouraging confidence across agencies in the new "responsibility to provide" environment.

## TAKING LESSONS FROM THE PRIVATE SECTOR

The government has previously been unwilling to invest in the technology required by some of these recommendations. However, the private sector has used many of these processes and technologies for years and had great success. In the financial and banking communities, many employees handle extremely sensitive financial information that can equate in sensitivity to many of our classified national security secrets. Examples of security-related systems in the commercial arena are applicable to the government's requirements.

Like the examples mentioned relating to the most damaging spy cases, the financial community has generally found that examples of fraud with employees do not occur during the first several months or years of an individual's employment, but instead happen as a result of evolving events that affect an individual's life. Thus, a system that only monitors an individual on a planned, periodic timeline cannot hope to identify growing risk in a way that can minimize damage and compromise—particularly when we know people will change jobs (and organizations) more frequently. Consequently, financial institutions have incorporated extensive systems of continuous monitoring of employees in order to ensure that any malfeasance can be identified and acted upon before significant damage can occur. In addition, a large portion of the financial sector's success in the security arena can be attributed to their incorporation of some of the key recommendations advocated earlier in this paper, such as:

- Financial institutions generally "clear" their employees in a matter of weeks. Afterward, the system focuses on a fully automated system of extensive record and database checks, revealing as much quality information as a field investigation, if not more so, and in a fraction of the time;
- Examples of reciprocity and continuous monitoring are found in the banking sector's federated credit card system. Banks and other

financial institutions authorize credit and debit cards based on an evaluation of one's suitability to have such a card. No matter where the card holder is, he does not have to find his bank to access his funds. Instead, a federated system enables financial institutions to recognize other institution's cards and provide ubiquitous access in real time. To illustrate this point, someone in Sydney, Australia can put their Visa Card into an ATM machine, where the data on the card is read and compared with a database of financial records. Once the legitimacy of the card is established, the system responds by allowing access to appropriate "funds." The individual could then withdraw significant amounts of money and walk away. In this scenario, the banking industry has taken on an element of risk. First that the individual has money in the account or has an available credit balance — information which is quickly ascertained by database checks — and second that the individual presenting the card is the legitimate card holder. To mitigate the second risk, continuous monitoring, running silently in the background, evaluates card usage and notes anything out of the ordinary, as defined by the card holders 'normal' usage. If suspicious behavior is detected, action is taken, usually in the form of a telephone call asking the card holder about recent purchases in order to confirm the spending or identify a breach in the security system. Most credit card theft can then be acted upon quickly.

- The financial industry implements a system of continuous monitoring of an individual's "credit score." An individual's ability to receive a loan to purchase a home depends, in large measure, on his credit score, which is established by continuous monitoring of his financial activities, and a subsequent evaluation of his suitability to receive the loan. The credit score, then, actually portrays a risk factor for a loan officer to use in adjudicating whether or not the loan will be offered. The credit score is continually updated and operates "in the background" on a regular basis. Consequently, an individual's score fluctuates depending on his activities and a basis of what is "normal" generally, with a loan officer also analyzing what is "normal" for the individual requesting the loan.

In all of these examples, systems exist that likely could be purchased, scaled, and modified for government use. This would, however, take a major commitment in terms of priority and funding.

# CONCLUSION

**As mentioned at the beginning of this report, for the first time senior leaders in the Department of Defense, the Intelligence Community, the White House, and elsewhere agree that there must be significant and dramatic change to the personnel security process. Collectively, they have embarked on a project to look at how to radically reform the current processes to create a system that meets the needs of today and tomorrow. INSA is highly supportive of this effort and hopes the recommendations in this paper will prove complementary to this effort.**

In any change to the system, there are two important points to keep in mind. First, the government should not look at this as a cost-saving effort. The new system can only be successful if it is fully resourced. This means that some of the resources saved from automation of the front end of the clearance process must be invested in the back end. That said, there will likely be significant savings to the government over time, including savings from reduced contract costs. Second, the government must avoid the tendency to utilize legacy systems to attempt to save costs or to prove that earlier expenditures were not in vain. Among other reasons, the time needed to modify new systems to conform to legacy systems would

delay needed change by years, if not decades. Many systems should be scrapped in favor of new, efficient ones.

By implementing the recommendations in this paper, the government can significantly improve our national security structure, including government, the private sector, and academia. Such changes will have an impact on many aspects of government operations and will undoubtedly create a more reliable and secure security structure for the nation, one capable of supporting our national security in a dynamic environment. INSA stands ready to assist the government in these efforts.



# APPENDIX A: CURRENT PROCESS BASICS

The concept of security clearances in the U.S. dates back to World War II and our need to protect sensitive information. The National Security Act of 1947 gave the authority and responsibility of granting access to classified information to the Executive Branch. A security clearance is essentially a determination that an individual is eligible for access to classified information. This is based on a rigorous investigation that explores most aspects of the individual's life in order to determine that the individual is trustworthy, loyal to the U.S., not a foreign agent, and does not have anything in his or her background that could be exploited by a foreign agent. The security clearance process relies on a front-end investigation, based on the above criteria, and once cleared the individual is not regularly re-investigated for at least five years. All agencies follow investigative and adjudicative standards set by a series of laws and executive orders, but may have additional policies and processes to meet individual needs.

## Decision Points

There are fourteen “decision points” on which a person's character and lifestyle are investigated and adjudicated when determining whether to grant access to national security information:

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Emotional, Mental, and Personality Disorders
- Criminal Conduct
- Security Violations
- Outside Activities
- Misuse of Information Technology Systems

## Clearance Process

The security clearance process can generally be broken down into four major pieces: Application, Investigation, Adjudication, and Reinvestigation. There is also a “requirements” process for determining which positions require clearances and at what level, and an “appeals” process should someone not be granted a security clearance.

**Application Submission:** Applicant completes and submits required documents, including an SF-86 and fingerprint cards.

**Investigation:** Agency, office, OPM, or contractor conducts investigation. The level of detail depends on the type of security clearance requested.

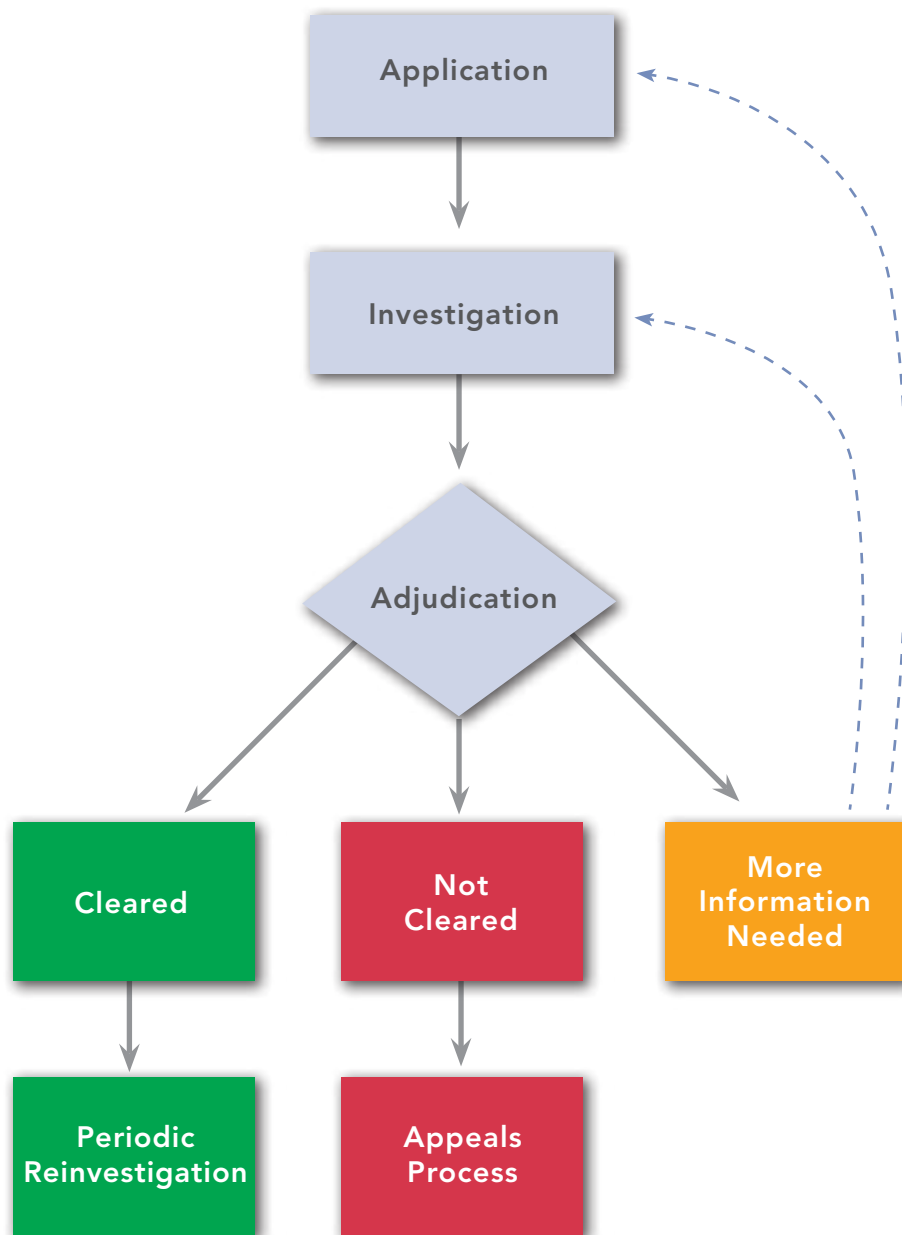
- **NACLC:** National Agency Check with Local Agency Check and Credit Check; requires local and national law enforcement history check and credit check. For use in CONFIDENTIAL and SECRET clearances.
- **SSBI:** Single Scope Background Investigation; requires NACLC plus verification of employment, educational, and residential history as well as interviews with the candidate and others. For use in TOP SECRET and TOP SECRET SCI clearances
- **Polygraph:** Test that measures physiological responses while candidate is answering questions.

**Adjudication:** Government office judges whether applicant is eligible for access to classified information.

See chart on following page.

APPENDIX A: CURRENT PROCESS BASICS CONTINUED

**FIGURE 1:** Current Security Clearance Process





# APPENDIX B: CURRENT SYSTEM VS. NEW SYSTEM FLOW CHARTS

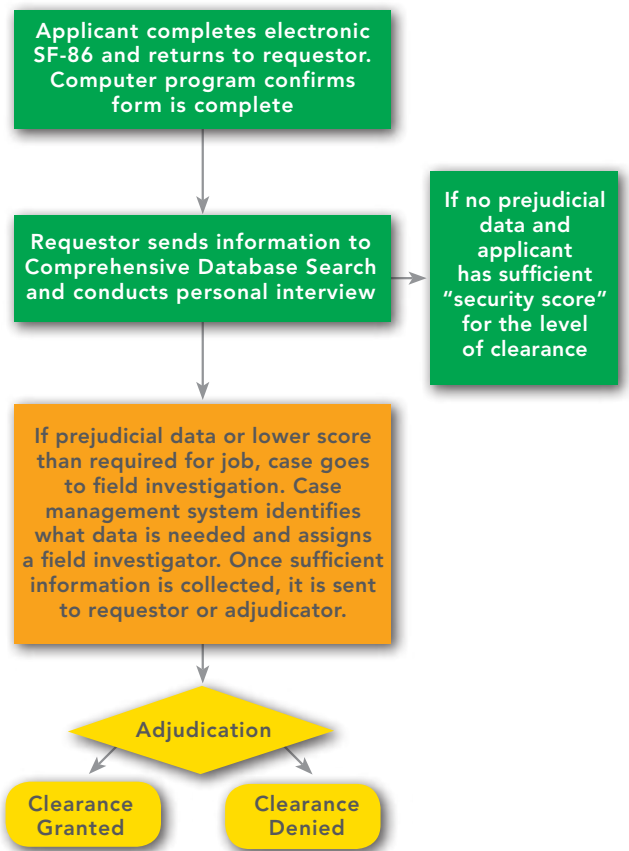
To better demonstrate how these six recommendations can improve upon the current system, below find two flow charts detailing the current and proposed processes.

**FIGURE 2: Current System vs. New System Flow Charts**

## GENERIC CURRENT SYSTEM



## PROPOSED SYSTEM





# APPENDIX C: HYPOTHETICAL CASES UNDER THE NEW SYSTEM

To better explain how the new system could function; follow the two hypothetical cases of Harry and Ralph through the clearance process and their careers. Harry is applying for a position at the DoD that requires a SECRET clearance. Ralph is applying for a position in a national intelligence agency that requires a TOP SECRET/SCI.

## Initial Clearance

**Harry and Ralph have their initial HR and Security interviews,** where an initial assessment as to their suitability for employment, including verification of standard data (education and employment data, for example) has taken place and is factored into the decision to hire each individual and submit them for the appropriate clearances. Both Harry and Ralph complete a standardized electronic applications process which includes supplying electronic fingerprints. As they fill out the online application, the system automatically indicates discrepancies in the input fields for critical information that must be addressed before the application can be electronically submitted, which eliminates the need for a quality review of the documents. Once submitted, the application goes to an electronic database for the automated records check, which is completed within a two week timeframe.

Harry's "security score" from this records check is 663, with no significant anomalies noted. The security officer has indicated that the acceptable "security score" for this position is 550 or above. Because Harry's score is acceptable, the automated system sends an adjudication message indicating that Harry can receive a SECRET clearance based upon this automated review. This information is then automatically incorporated into Harry's file, and Harry can begin work immediately. Had Harry's "security score" been lower than 550, the computer would

send the file to an adjudicator who would consider whether to order a full or partial field investigation to gather more information before adjudicating on Harry's case.

Ralph's "security score" from the database check is 980; well above the 800 score necessary for his position. However, given the sensitive nature of the job, the security officer indicated at the beginning of the process that at least a partial field investigation is required. The results of the automated check are sent to an adjudicator, who, upon review of the case, electronically sends the case to several field investigators simultaneously, with any special instructions and deadlines for completion of the work. In the field, each relevant investigator has received an electronic message that a new case file has been assigned. The investigators use their secured laptop computers to access a special web-based database containing the case file and necessary elements to be investigated. The investigators conduct their investigations simultaneously, entering the results into the case files and electronically sending the results to the adjudicator. Because the system incorporates technology, case managers can monitor workloads and electronically reassign tasks and cases to most efficiently use resources. Once the information is received from the field by the adjudicator, it is determined that Ralph is suitable and trustworthy for the sensitive job for which he has applied. The clearance is granted and Ralph and his security officer are notified.

## Mid-Career

**One year later, Harry's "security score" spikes** to 900. The automated records check indicates that the reason for such a change is based on a sudden change in financial status with a significant influx of available cash that is not a result of Harry's

## APPENDIX C: HYPOTHETICAL CASES UNDER THE NEW SYSTEM CONTINUED

investments. A message is sent to an adjudicator who assesses the information and can decide to contact Harry's security officer and request that he hold an interview with Harry, or an aperiodic investigation. Given Harry's current job and access, the adjudicator requests the interview. Harry's security officer determines in the interview that Harry's wife, who writes children's stories, has recently received a significant advance for a new book. The adjudicator requests verification of this information and upon receipt notes this anomaly in Harry's records, with no further action required. Six months later, Harry decides to apply for a new job in a different agency of the government. This job also requires a SECRET clearance, but the "security score" range is set at 850. Harry's "security score" has stayed at the 900 level. Upon checking the database, the new security officer notifies management that, from a security standpoint Harry can start work the next day.

### THREE YEARS LATER, RALPH'S "SECURITY SCORE" SUDDENLY DROPS CONSIDERABLY TO 650. GIVEN THE NATURE OF RALPH'S WORK, AN APERIODIC INVESTIGATION IS INITIATED.

Two years after his initial clearance is received, Ralph is notified that an aperiodic investigation is going to be conducted and is requested to review, update, and submit a new electronic application. He submits the information and within 60 days is notified that the investigation is complete with no adverse information collected. Three years later, Ralph's "security score" suddenly drops considerably to 650. Given the nature of Ralph's work, an aperiodic investigation is initiated. Upon review of the data from the automated records check, it is clear that the reason for the change is a sudden change to Ralph's financial status. During the investigation, it is learned that Ralph and his wife have just bought a house that they had been eyeing for years, but required using most of their available cash and considerable investments. It is determined that a security risk does not exist and the case is updated and closed.

### Exiting Government

**A year later, Harry decides to leave government** and go into the private sector. The job that interests him the most requires a TS/SCI clearance. The corporate security officer queries the database and discovers that Harry's "security score" continues to be around 900, while the job requires a minimum of 800. Upon certification that the security information is correct, Harry can start work immediately with a TS/SCI, provided that the necessary indoctrination is conducted by his new corporate security officer.

Five years later, Ralph decides to retire. At the moment, he has not decided whether to do private consulting, work for a corporation, or teach at a nearby university. The latter job requires no clearances. Ralph decides to take the teaching position. Upon retirement, he is given the option of staying in the security system and remaining subject to continuous monitoring and aperiodic investigations, or opting out of the system, with the requirement to start the process over in the event that later on he has a job requiring a security clearance. Ralph decides to stay in the system. Two years later, Ralph decides to augment his teaching with some private consulting contracts that include access to classified information. The security officers involved query the database and discover that Ralph has been maintained in the system with a good "security score" and can begin work immediately.

### Conclusion

**In both cases there is a heavy reliance on the** automated application process and on the automated records check process to speed up the initial clearance. Because automation is a more effective and efficient use of human resources, adjudicators and field investigators are free to concentrate on critical components and counterintelligence. In addition to freeing up resources to do robust counterintelligence, this system also provides deterrent against those considering harming national security through constant monitoring and aperiodic investigation.

# APPENDIX D: ABOUT THE INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

The Intelligence and National Security Alliance is a not-for-profit, non-partisan, professional association created to improve our nation's security. As a unique forum where the once-independent efforts of intelligence professionals, private sector leaders and academic experts can come together, INSA is identifying the critical issues facing our nation's security in the decades to come. Through symposia, white papers, and debate, INSA's members are laying the intellectual foundation to build the Intelligence Community of the 21st Century. Through education, advocacy, and open programs, INSA is working to inform the broader public and inspire the workforce from which the leaders of the next generation will rise.

## INSA's Council on Security and Counterintelligence

**The Council on Security consists of high-ranking current and former private sector and government officials who have a vast array of knowledge of security issues and processes. The Council provides progressive solutions to improve**

existing security policies and take advantage of cutting-edge technologies in both sharing and safeguarding information. This group is working in concert with the government in order to both improve and restructure security clearance processes as well as other aspects of security policy and programs to ensure information integrity and secure operations in intelligence and national security.

This paper is a product of the INSA Council on Security and Counterintelligence. Those serving on the Council do so as individuals in their own right and the views presented in this paper do not necessarily reflect the views of all individual and corporate INSA members.

Tim Sample  
*President, INSA*

Hannah Powell  
*Director of Research and Analysis, INSA*







INTELLIGENCE AND  
NATIONAL SECURITY  
ALLIANCE

**INTELLIGENCE AND NATIONAL  
SECURITY ALLIANCE**

Ballston Metro Center Office Towers  
901 North Stuart Street, Suite 205  
Arlington, VA 22203  
Phone (703) 224-INSA  
Fax (703) 224-4681