



THE STATE OF THE SECURITY CLEARANCE PROCESS:

HOW WE GOT HERE AND
WHERE WE'RE GOING

BY MERTON W. MILLER, FORMER DEPUTY DIRECTOR, NATIONAL BACKGROUND INVESTIGATIONS BUREAU (NBIB)

In spite of a lengthy and complex investigations process, there has been a recent wave of cleared personnel committing crimes and violating the public trust. To name a few: Nidal Hasan (DoD), Chelsea Manning (DoD), Harold Martin (NSA), Kun Shan Chun (FBI), and perhaps most notoriously, Edward Snowden (NSA). The charges against leakers include spying, murder, support of terrorism, and leaking classified information—among many others.

Unfortunately, this problem isn't new, but the high-profile nature of these breaches has forced the government to act. As it has looked to address insider threats like these, a new layer of problems has emerged. There is a 700,000 case backlog of pending investigations, a 534 day average timeline to issue a Top Secret security clearance for DoD contract employees, and for the first time since 2011, the Government Accountability Office has put the security clearance process back on the High Risk List.

This paper looks at the current backlog in the clearance investigations process, how we arrived here and—most importantly—what must be done to start fixing the background investigative process and restoring our national security.

The Current State of the Background Investigative Program

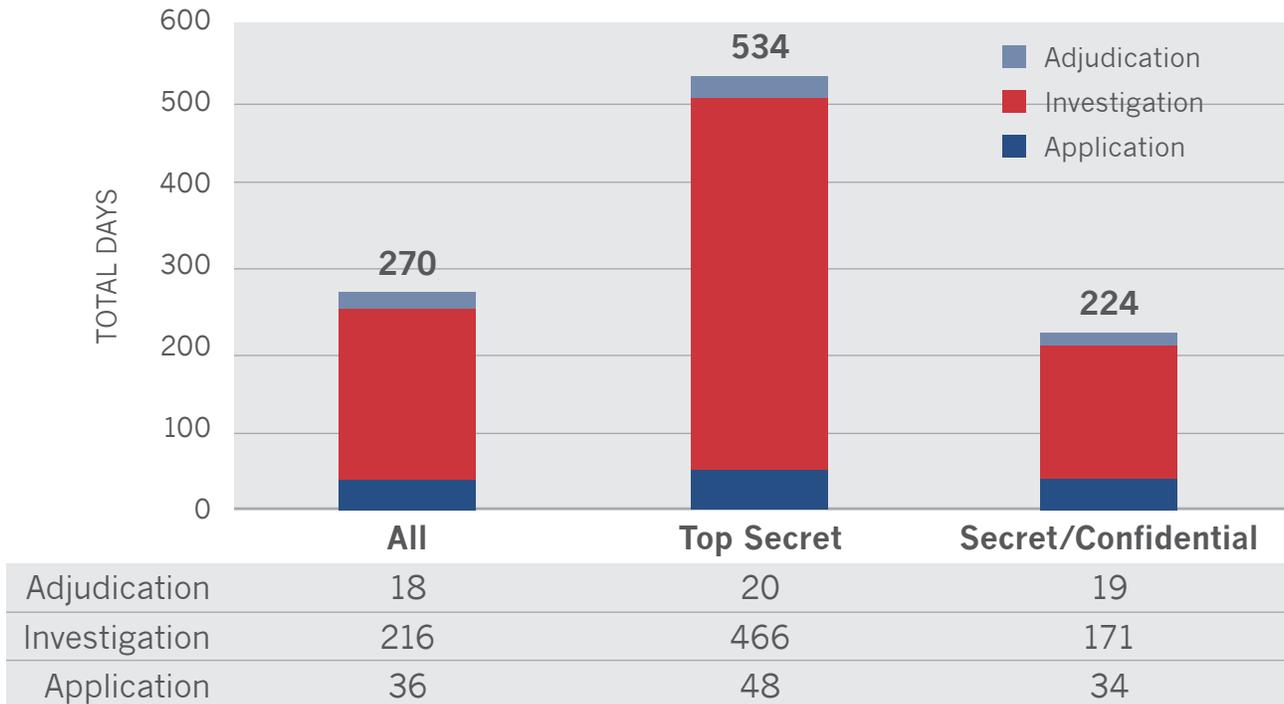
As former Associate Director for the Federal Investigative Services (now National Background Investigations Bureau [NBIB]), I observed firsthand how the federal government's inconsistent approach to managing the background investigations program has delayed and disrupted any attempt at program improvement. Background investigations should be viewed as one of the most important steps the federal government takes to protect our national security from insider and external threats. The frequency of counterintelligence, terrorism, and other serious issues identified through initial and periodic reinvestigations reinforces how essential the background investigation program is to national security.

Perhaps one of the greatest issues within the personnel security program is the lack of consistency. The same policy has governed the national security establishment since 1947. However, political inclinations, agency

disagreements, and contract changes have created a situation where progress gained quickly becomes progress lost. To put the numbers in perspective, in Fiscal Year 2014, the normal investigative workload averaged approximately 160,000 cases. Secret investigations took 28 days and Top Secret investigations took an average of 77 days to complete. Currently, there are more than 700,000 background investigations pending in the NBIB inventory, the average Secret investigation takes 132 days, and Top Secret investigations take 323 days to complete across all of government—including military personnel, direct government employees, and contractors.

Unfortunately, more than half of the pending investigations are in limbo due to the lack of available investigative resources, and approximately 194,000 (28%) of the pending cases are "periodic reinvestigations" for federal employees and contractors already in access.

Clearance Processing Times for DoD/Industry



Source: National Background Investigations Bureau.

What are the effects of background investigation delays?

The results of the current crisis play out in three key ways:

1. National Security is Compromised

In September 2013, Aaron Alexis killed 12 and injured three others in a mass shooting at the headquarters of the Naval Sea Systems Command (NAVSEA) inside the Washington Navy Yard. Following the shooting, the White House initiated a 120-day review resulting in several recommendations to enhance national security. The report identified 13 major conclusions and recommendations, which aimed to achieve three broad goals:

- Increase availability of critical information
- Reduce inherent risk in current processes
- Improve enterprise operations

Four years later, the majority of those recommendations have yet to be implemented. A proposal to reduce the 10-year reinvestigation standard to five years for individuals with Secret clearance still has not been implemented. (It's worth noting that since Alexis' clearance was adjudicated in 2008, he was not due for a reinvestigation until 2017). In addition, because of the backlog, the reinvestigation timeline for Top Secret clearances has been increased to six years.

When the Navy Yard incident was in the national spotlight, gaps and risks in the investigative process became a top priority. However, once they became an inconvenience, standards were compromised.

2. Government Effectiveness Is Reduced

Background investigations are required for all federal employees and contractors considered for positions of national security and public trust. When these investigations are delayed, it severely impacts federal agencies and contractors in hiring and filling critical positions. This hampers government's ability to effectively operate and provide services to the American people. Currently the government is lacking the number of cybersecurity specialists, customs and border patrol agents, intelligence analysts, engineers, accountants, doctors and nurses, and even background investigators to operate as effectively as it should. Today, almost every federal agency is experiencing serious mission impacts because of the investigative backlog.

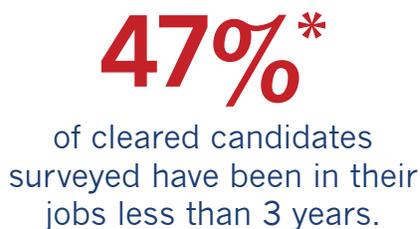
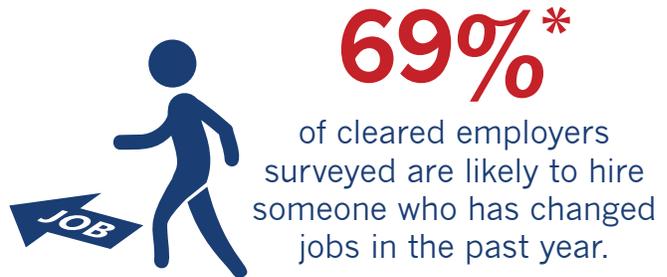
“ What the metrics fail to capture are the real-world impact of the backlog—the new careers put on hold, top talent lost to non-defense industries, and programs that provide critical warfighter capabilities delayed with cost increases. The delays also come with a real-world price tag.

—Jane Chappell, Vice President of Global Intelligence Solutions, Raytheon

3. The Government Loses the Best Qualified Candidates

Background investigation and adjudication delays drive highly qualified candidates to search for work outside of government service. Realistically, many job candidates cannot afford to wait over a year for their clearance to materialize. What's more, decreases in investigative timeliness cause an unhealthy shift in the hiring approach of industry and the federal government. Finding candidates who are *already* cleared is now the priority, and although skills and qualifications are also important, they're less of a priority.

As a result, the talent pool becomes so limited, government and contract employers are left poaching from each other in order to hire talent. Qualified professionals are inundated with offers and job hopping becomes the norm. This is both costly financially and to our national security.



*According to a 2016 survey by ClearanceJobs.com.

Backlogs, Delays, and Cost Overruns...How Did We Get Here?

Backlogs in the Personnel Security Investigations (PSI) program have existed since as early as 1986, when DoD had more than 300,000 overdue reinvestigations. This backlog remained through 2002 when a House Committee report estimated the investigative backlog ranged from 350,000 to 900,000 cases. During this same period, Defense Security Service (DSS) data showed that it was taking an average of 403 days to complete “initial” Top Secret investigations and an average of 470 days for Top Secret periodic reinvestigations.

There were multiple comprehensive reviews to address this backlog and reform the investigative process. Review after review was met with the same result: the backlog continued to grow and national security remained at risk. Despite repeated recommendations by the Government Accountability Office (GAO) and promises by DoD to grow the investigative staff and increase funding to support the PSI program, DoD cut staff and underfunded the program.

In February 2005, two important events took place that would change the course of the PSI program and lay the foundation for the current situation. First, GAO designated the DoD personnel security clearance program as a high-risk area. Language in the GAO report specifically stated:

“ Negative effects of delays in determining security clearance eligibility are serious and varying depending on whether the clearance is being renewed or granted to an individual for the first time. Delays in renewing previously issued clearances can lead to heightened risk of national security breaches because the longer individuals hold a clearance, the more likely they

TIMELINE OF EVENTS

OPM's Investigation Program

- **1994** OPM's investigation program identified for privatization by the Clinton Administration.
- **July 4, 1996** An employee stock-owned company is formed consisting of former OPM employees—U.S. Investigations Services (USIS).
- **December 2004** Intelligence Reform and Terrorism Prevention Act (IRTPA) sets timeliness standards for security clearance determinations.
- **January 2005** GAO designates DoD's personnel security clearance program as a high-risk area.
- **FEBRUARY 2005** DSS transfers its personnel security function and about 1,600 personnel to OPM.
- **June 2005** Executive Order 13381 designates the OMB as the element of the executive branch responsible for oversight of all investigations and adjudication for personnel security clearances. OMB then **designates OPM as primary investigative agency** for conducting security investigations in the federal government.
- **June 2008** Executive Order 13467 names the Security and Suitability Executive Agent, and establishes the Performance Accountability Council, responsible to the President, to drive implementation of the reform effort.
- **August 2008** OPM announces its ability to provide total end-to-end electronic processing of investigations.
- **January 2011** GAO removes DoD clearance program from its high-risk list based, in part, on the improved timeliness of investigations.
- **October 2012** The Director of National Intelligence—in his role as Security Executive Agent—set a new government-wide goal for Top Secret clearances (80 days for investigation and 20 days for adjudication).
- **December 2012** The Suitability and Security Executive Agents sign the revised Federal Investigative Standards.
- **February 2014** OPM fully federalizes quality review process.
- **February 2014** Suitability and Security Processes Review, Report to the President, issued following the Presidentially-directed 120-day study.
- **MARCH 2014** A cyberattack allows access to an OPM automated system. No loss of personal information is identified.

are to be working with critical information and systems. Delays in issuing initial clearances can result in millions of dollars of additional costs to the federal government, longer periods of time needed to complete national security related contracts, lost-opportunity costs if prospective employees decide to work elsewhere rather than wait for the clearance, and diminished quality of the work because industry contractors may be performing government contracts with personnel who have the necessary clearances but are not the most experienced and best qualified personnel for the positions.”

These same challenges (clearance delays, added costs, competition for talent) repeat again, beginning in FY 2014.

Second, the Office of Personnel Management (OPM) assumed responsibility for all DoD personnel security background investigations, including the 144,000 investigations in progress with DSS. Operational control of 1,600 DSS staff and first-line supervisors dedicated to the PSI mission transferred to OPM. During the transfer, Paul Wolfowitz, Deputy Secretary of Defense, related:

“the proposed transfer of function would improve the timeliness of investigations and leverage the success that OPM and the private sector ha[ve] achieved over the last several years in this area. The transfer would allow DoD to concentrate its efforts on other security functions, which are part of the Department’s core mission responsibilities.”

By February 2009, the PSI program was finally current for the first time in decades. This success was thanks to two key moves. Firstly, four years of aggressive growth of the federal and contractor background investigative staff to more than 8,000 people. Secondly, proper funding through the OPM revolving fund (a fee-

- **SEPTEMBER 2014** OPM’s contracting officer informs USIS of the decision not to extend the term of its contracts for both background investigations and support services.
- **September 2014** FIS notifies agencies it increased prices to ensure that it recoups the costs necessary to run OPM-FIS’ investigation program.
- **February 2015** GSA concludes its prospectus-site study, and recommended the construction of a new federally-owned facility for the OPM and other federal tenants in the vicinity of Boyers, PA.
- **JUNE 2015** OPM becomes aware of intrusions into its systems in April (affecting personnel records) and May (affecting background investigations data) after implementing new measures to deter and detect cyberattacks.
- **JULY 2015** OPM announces that in the second cyber breach, SSNs for 21.5 million individuals and 5.6 million fingerprints were stolen.
- **January 2016** The Administration announces that it will establish a new government-wide service provider for background investigations, the National Background Investigations Bureau (NBIB), which will be housed within OPM.
- **OCTOBER 2016** NBIB becomes operational.

for-service model), the PSI program finally had the resources it needed to successfully meet the government’s investigative requirements and exceed congressional timeliness mandates. In February 2011, in recognition of this milestone, GAO removed the DoD Personnel Security Clearance program from its high-risk list. From 2009 through 2014, the OPM Federal Investigative Services (FIS) continued to meet and exceed Congressional Intelligence Reform and Terrorism Prevention Act (IRTPA) timeliness mandates—28 days for Secret, 77 days for Top Secret, and 38 days for 90% of all initial investigations—and kept investigative costs flat (less than 3% increase over a five-year period).

While not perfect, 2009 through 2014 arguably represented the most successful period of performance during the long-failed history of the PSI program.

The Perfect Storm

After this encouraging progress, in 2014, the background investigations program experienced the “perfect storm” that would eventually lead to the current backlog. The OPM cyber breach, DoD’s failure to properly estimate workload, and the decision not to extend the largest investigative provider contract, resulted in the current backlog—increasing costs, and amplifying risk to national security.

Some history is necessary to understand the significant events leading to the shortfall of investigative staff and funding to support the PSI program in late 2014. In 1996, under the Clinton Administration, a decision was made to privatize the background investigations program. Under the privatization plan, the OPM investigation office’s functions were transferred to a new company created by the federal government called U.S. Investigations Services (USIS). The company was granted a non-compete, sole-source contract to perform background checks for OPM for three years. Following the expiration of the three-year “no compete” period, USIS had to compete with other private services.

As the investigative program expanded and OPM took over the DoD PSI work, the government’s dependence on USIS grew. In FY 2014, the distribution of background

investigative work between federal investigators and contract investigators was approximately 30% federal and 70% contractor. Of the 70% of investigative work performed by contractors, USIS accomplished 60 to 65%. In addition to providing the majority of the contract investigators for the government’s background investigative program, USIS also provided the most competitive pricing to the government for investigative services. Bottom line: The U.S. Government relied heavily on USIS to provide a significant number of investigative man-hours to meet government-wide investigative demands.

The government made the decision to stop issuing new investigations to USIS in August of 2014, shortly after the company acknowledged a data breach which compromised the private data of security clearance applicants. The cyber breach was the final straw in a series of federal government criticisms of USIS, including allegations of falsified reports and a Department of Justice complaint. OPM cancelled the contract in September of 2014. **This decision resulted in the loss of 65% of the government’s investigative capacity in just a one-month period.** This move created three main challenges, from which the government is still trying to recover:

CHALLENGE #1: FEWER INVESTIGATORS, HIGHER COSTS

Simple math showed that the loss of the USIS contract resulted in increasing contract costs by approximately \$100 million annually. USIS had always been the lowest cost investigative services provider. The cost difference between USIS and the new contract investigative service providers resulted in overall investigation costs going up by 43.5%. When the USIS contract was cancelled, there were simply no other investigative providers who could offer the same scale and cost effectiveness. In addition, the loss of approximately 3,000 contract investigators resulted in a daily shortfall of over 24,000 man-hours to tackle current investigative workload. The program immediately fell into a critical revenue and manpower shortfall situation.

CHALLENGE #1: FEWER INVESTIGATORS, HIGHER COSTS (Cont'd)

OPM's response compounded the crisis. Beth Cobert, OPM's new acting director, asked Office of Management and Budget (OMB) to conduct a study to assess Federal Investigative Services (FIS) finances and asked the FIS staff to find program efficiencies to replace the millions of lost USIS man-hours. This new requirement came as the government was already scrambling to make up for the lost investigative hours.

Consequently, the background investigative program fell further and further behind. To make matters worse, because monthly expenses were far exceeding revenue, FIS was losing money at a rapid rate. The rate of FIS financial losses and the uncertainty of when, or if, OMB would recommend an increase in revenue for FIS created serious uncertainty. It also suspended any internal initiatives—like overtime, increased federal hiring, surge contract, new IT solutions, etc. to try to slow the growth of the investigative backlog.

Almost one year after the loss of USIS, OMB and OPM leadership agreed an immediate price increase was necessary. FIS was literally just a few short weeks away from not being able to pay its bills when OMB and OPM leadership agreed to initiate a retroactive price increase. The retroactive price increase meant that every OPM background investigative customer would receive a bill charging them more than the originally agreed upon price for all investigative work submitted in FY 2015. Had the price increase been implemented at the beginning of the fiscal year, government agencies would have been able to manage their investigative costs more effectively. As OPM FIS performance declined in delivering timely background investigations, and the backlog grew by almost 75%, each customer received a bill from OPM during their end of fiscal year close out. DoD's portion of the bill alone was over \$92 million.

TIMELINESS OF NATIONAL SECURITY INVESTIGATIONS

Investigation Type	FY 2005	FY 2014	FY 2015	FY 2016	FY 2017
All Initial Investigations	145 days	35 days	87 days	123 days	158 days
Top Secret/Q	308 days	75 days	147 days	220 days	323 days
Secret/Confidential/L	115 days	30 days	56 days	108 days	132 days
Reinvestigations	418 days	117 days	197 days	219 days	302 days

FY 2005 – Program officially transferred from DoD to OPM

FY 2014 – OPM meeting IRTPA standards (2009-2014)

FY 2015 thru June 2017 – Timeliness growing month over month and continuing to trend up

Source: Office of the Director of National Intelligence.

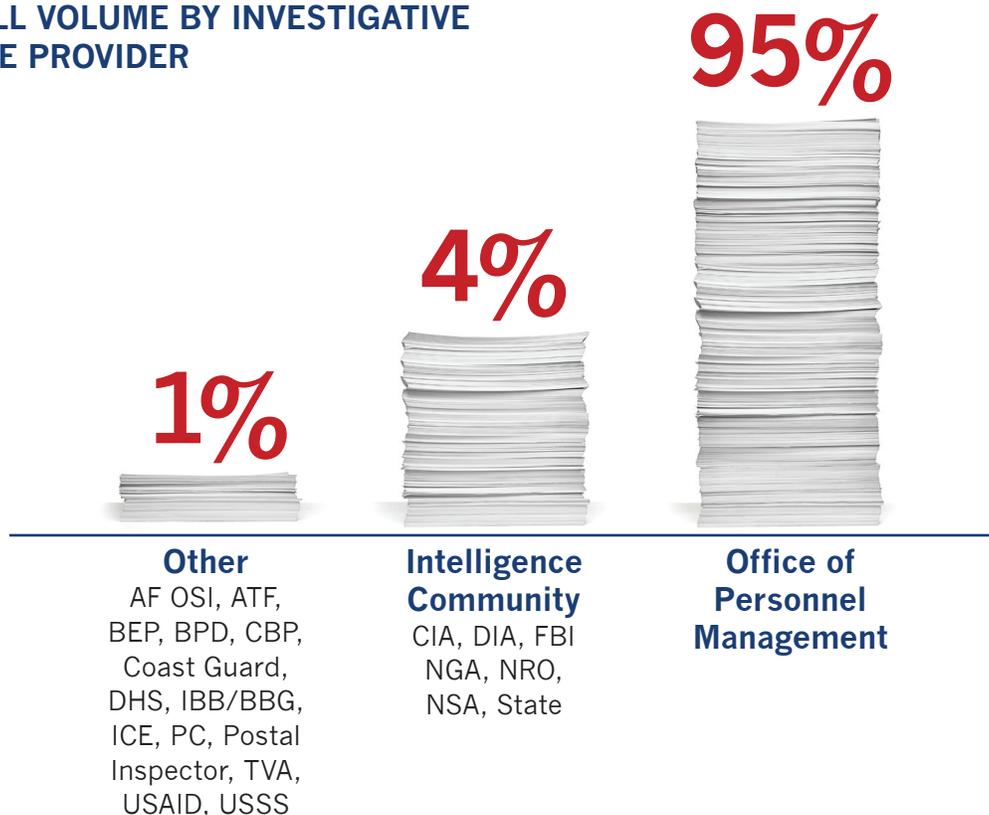
CHALLENGE #2: ADDRESSING THE OPM BREACH

Following the OPM breach in 2014, the White House initiated a 90-day Suitability and Security review of the background investigative program. The review was intended to identify reforms and determine improvements to the way the government conducts background investigations. The review resulted in a proposal to replace the FIS with a new agency, the National Background Investigations Bureau. The primary change was to create a political head for the organization, which still reported to OPM.

Some 190 days after the initiation of the 90-day review, the Administration announced its findings and intended steps to improve the government's security clearance and background investigation processes for Federal employees and contractors:

“ These actions include establishing a new federal entity (NBIB), which will strengthen how the Federal Government performs background investigations. The actions will also assign the Department of Defense (DoD) responsibility for the IT security of and data related to the background investigations systems for the new entity. These actions will create a more secure and effective Federal background investigations infrastructure.” –White House 90-day review

OVERALL VOLUME BY INVESTIGATIVE SERVICE PROVIDER



CHALLENGE #3: THE GROWING COST OF PERSONNEL SECURITY

As the backlog grew, the cost to address the problem grew, as well. There was a limited number of background investigators available across the federal government and industry. What’s more, the additional resources needed would not be available overnight. The timeline to increase federal investigators capable of independently conducting fieldwork was a minimum of six months (after five weeks of initial training.) Along with training new contract investigators, eliminating USIS meant the need for a new contract, creating additional delays as it went through the lengthy federal government competitive procurement process.

The GAO has conducted numerous studies of the background investigations program over the past three decades. **One GAO study claimed that every day a person is delayed being cleared for government service costs the government \$250.** At the time of the study, the average investigation took approximately 145 days. In 2004, through the Intelligence Reform and Terrorism Prevention Act, Congress mandated that the top 90% of all background investigations not exceed 40 days.

By 2009, OPM had met the timeline established by Congress. In fact, if one used the figures from GAO’s study, over an eight-year period, improved investigative timeliness would be saving the federal government over \$26 billion¹. Unfortunately, the current state of the background investigative program has reversed the billions of dollars of efficiencies and cost avoidance trend.

COST OF BACKGROUND INVESTIGATIONS

Standard Handling	FY 2017	FY2018	Increase+
Tier 1 (Low Risk-no clearance)	\$176	\$194	\$18
Tier 2 (Moderate Risk-Public Trust)	\$1,515	\$1,550	\$35
Tier 2R	\$1,204	\$1,261	\$57
Tier 3 (Noncritical Sensitive-Secret)	\$421	\$433	\$12
Tier 3R	\$397	\$417	\$20
Tier 4 (High Risk-Public Trust)	\$4,051	\$4,218	\$167
Tier 4R	\$2,565	\$2,646	\$81
Tier 5 (Critical or Special Sensitive – Top Secret and/or SCI)	\$5,389	\$5,596	\$207
Tier 5R	\$2,951	\$3,065	\$114

Source: Investigative Notice (FIN) 17-04.

¹Using GAO’s \$250 per day and applying the savings across the annual background investigative workload of 2.2 million investigations over an eight-year period.

How Can We Reverse the Background Investigation Backlog and Improve National Security?

The security clearance storm is still brewing, but all hope is not lost. While the security clearance program's reinstatement to the GAO high risk list may seem like a step backward, it has had its benefits. It has increased congressional attention to security clearance reform and steps are being taken to improve personnel security.

Here are three steps the government could take to improve the function of the background investigations program, increase timeliness, and advance national security:

Establish an Independent Agency (IA)

Government-wide centralization of the background investigative program has proven, time and again, to be the best, most efficient, and cost-effective approach for managing and advancing the background investigations program. The creation of the NBIB was a stop-gap measure, but fails to accomplish the same efficiencies one would see in an independent agency. By establishing an IA, the federal government would finally put in place the structure necessary to focus on this important national security function. The IA would:

- Safeguard and advance government-wide governance, control, and performance accountability;
 - Ensure program costs are appropriate, balanced, and transparent across the federal government;
 - Deliver program-wide IT strategy and outline system requirements and system development (case management should be first priority);
 - Advance standards for and centralize information collection, documentation, and records management;
- Establish and maintain program-wide quality and training standards; and
 - Oversee the structure, validation, and integration of automated record checks, and align investigative activities to support government-wide continuous evaluation (CE) and insider threat efforts.

Advancing Background Investigations

There has always been a great deal of discussion about changing the background investigative process, because it has not changed since it was first established in 1947. Even if policy does change (which is a slow and arduous process), background investigations will always require the collection, validation, analysis, documentation, dissemination, and adjudication of relevant information about the subject to determine their character, conduct, and fitness for federal service.

To advance the current investigations program we should concentrate on:

- Improving data collection methodologies (search engines, automated collection, direct connect, interactive surveys, and investigative interviews);
- Enhancing accessibility, reliability, and completeness of background investigative records, information, and data sources;
- Advancing analytical procedures (predictive, prescriptive [data-mining], and diagnostic) to support investigative and adjudicative activities;
- Increasing the rate and frequency of background collection (periodic reinvestigations, event-driven, continuous evaluation, periodic queries, continuous monitoring [the FBI Rap Back program], etc.)

- Converting investigative information into formats to enhance and streamline investigator, reviewer, and adjudicator roles and responsibilities.

Improve Investigative Technology with a Modern Case Management System

If there were only one new system that could be implemented in the next five years to support the background investigations program, the first priority should be on the implementation of a modern, centralized case management system. The current case management system used by NBIB, the Personnel Investigations Processing System (PIPS), severely limits their ability to make important collection, process, procedural, performance, transparency, oversight, and contracting model changes to the background investigations program.

The implementation of a modern case management system would give the federal government the capability to reduce the backlog much more quickly, improve timeliness, reduce costs, and most importantly, reduce the risk to our national security. Security clearance reform today highlights the continued gaps in implementing reciprocity across government agencies. The lack of a modern case management system is responsible for creating many of those gaps.

A modern case management system would allow us to:

- **Increase the operational and contracting model to expand investigative resources, save costs, enhance efficiencies, and target investigator expertise.** A modern case management system would allow workload assignment at the “item” (lead) level opening the door for geographically limited companies to compete for certain “types” of

investigative work. For example: a company in Chicago could compete to provide criminal history record information (CHRI) from law enforcement agencies who do not contribute CHRI information to the National Law Enforcement Telecommunications System (NLETS) or a state-wide system.

- **Increase “End to End” investigative efficiency and productivity.** Increase process efficiency by eliminating current error-prone manual aspects of the application and case management process by automating data capture, validation, and documentation.
- **Share relevant information across investigative functions.** A robust, scalable and flexible enterprise case management system would capture and share relevant investigative information across functions (field collection, documentation, validation, quality review, documentation, and dissemination) in a safe and secure environment.
- **Ensure investigation accuracy.** A modern case management system would provide automated validation and detection of missing or incorrect investigative information enhancing processing, reducing costs, and ensuring only accurate and complete data enters the electronic investigative record.
- **Improve collaboration, transparency, and customer service for investigative customers.** Enable effective and efficient collaboration across multiple government customer agencies to support investigative submissions, provide near real-time investigative status updates, and notify customer of issues as they develop.
- **Improve data access, compatibility and collaboration.** Promote data portability, collaboration, and allowing information to be viewed by internal and external users with appropriate permissions throughout the investigative and adjudicative process.

Finding a Better Path for Personnel Security



If one thing is certain, *personnel security is national security*. Just as it was in 2004, the PSI program today is at a critical juncture. A focus on true reform and program improvements will have an immediate effect on both government cost, program efficiency, and national security. What the personnel security program requires today is the realization of meaningful government-wide improvements to stabilize costs, reduce duplication, meet timeliness mandates, standardize quality, increase government efficiency, and improve reciprocity.

The bad news is, the system is broken. The good news is, we've fixed it before.

Merton W. Miller is a retired Colonel and Federal Agent with the Air Force Office of Special Investigations, and former Senior Executive with the Federal Investigative Service and National Background Investigations Bureau. His assignments included tours as Security Advisor White House Military Office, Assistant Director Office of the Secretary of Defense Counterintelligence, Commander AFOSI Region 6, Director Counterintelligence Field Activity Counterintelligence Campaigns, Associate Director for the Federal Investigative Services, and Deputy Director for NBIB.