

September 1, 2007

VIEWPOINT

Secret of Success

A risk-based approach could unplug security clearance backlogs once and for all.

BY JOHN
CASCIANO



Since 1974, the Government Accountability Office has published no less than 74 reports on issues plaguing the federal security clearance process—the most recent was released in September 2006. The messages and recommended solutions have been remarkably consistent. Yet more than three decades after the first report, the clearance process still suffers from many of the same problems, as witnessed by an estimated backlog of roughly 180,000 cases at the Defense Department alone.

Procedures for investigating and adjudicating security clearance applications are founded on a largely paper-based system that dates back to World War II. Backlogs and delays cost the government as much as \$1 billion in lost productivity every year, and they prevent the government and contractors from hiring people who are desperately needed in the war on terror.

Fortunately, there is new momentum for a solution. Director of National Intelligence Mike McConnell and James Clapper, undersecretary of Defense for intelligence, recognize that in order to stem the detrimental effects on national security, this anachronistic system

must be reinvented. In his recent One Hundred Day Integration and Collaboration Plan, McConnell said the intelligence community must “build on best practices in risk management.”

The national security community must look to existing commercial technologies and data to transform the process from one of risk avoidance to risk management. The clearance process treats all incoming cases the same, resulting in time-consuming deliberations, routine investigative methodologies and a disproportionate amount of human resources dedicated to investigating low-risk applicants. In contrast, a risk management approach would provide timeliness, adaptability, predictability and effectiveness without sacrificing security. It begins by taking advantage of available, affordable and proven technology to pre-screen applicants and segment the pool by risk level.

But technology on its own is not the silver bullet. Some in the national security community advocate a complete overhaul of the process, while others want to pursue goals that can be achieved quickly at minimal cost. The answer lies in a combination of the

two approaches. It is possible to make critical near-term improvements while reengineering the entire process. Technology and data can help investigators and adjudicators more effectively target and prioritize investigations.

The security clearance backlog can be addressed immediately by leveraging commercial technology, analytics and data in four pivotal areas:

- Electronic verification of information on applicants' Standard Form 86.
- Risk segmentation and pre-investigation of applicants for more effective allocation of investigative resources.
- Case management software to enhance the monitoring and visibility of investigations.
- A persistent reinvestigation process that can be triggered by automatically flagging high-risk or derogatory information contained in public and government records.

Electronic Verification

The initial identity verification and background screening process begins with a fundamental questionnaire, the SF 86. By using available technology and open source records, the government could electronically verify more than half the fields in the SF 86, such as name, address, date of birth, telephone number, Social Security number, within seconds. This automated process would be a vast improvement over today's laborious and time-consuming manual process.

Risk Segmentation

Commercially available risk scoring technologies, such as those used by the financial services sector, could be applied to commercial data, public records and government data sources to more effectively segment the pool of applicants according to their associated risk.

Once the relevant data are fused and analyzed, investigators can assess a composite risk score. Automating risk assessments to confirm basic applicant information conserves valuable labor. Investigators can prioritize high-, medium- and low-risk subjects, assigning the most senior investigators the highest priority and most ambiguous cases. This would shorten processing times.

In addition, by analyzing public records through investigative tools similar to those used by law enforcement agencies across the country, investigators could develop leads to guide their interview process, rather

than squandering time and resources on routine interviews with neighbors, relatives and associates listed on an applicant's SF 86. Advanced link analysis and social networking tools could lead investigators to associates that weren't volunteered on the SF 86.


Visibility of Investigations

GAO recently reported that it takes an average of 446 days to process initial clearances and 545 days for reinvestigations. These numbers fall well short of the 120-day goal in the 2004 Intelligence Reform Act. Part of the problem is investigators and adjudicators lack real-time visibility into the status of cases during the process. A case management system could automatically push alerts and updates to the investigating and adjudicating agencies through a digital dashboard as soon as the status of an investigation changes.

Persistent Reinvestigations

Public data, when fused with information held by government agencies, can improve the reinvestigation process. When case data can be matched electronically against public records, investigators can more efficiently track and analyze changes to personal information and uncover facts that might spark an immediate reinvestigation, such as arrest records, bankruptcies or "unexplained influence"—for example, when a CIA spy drawing a GS-14 salary buys a new Jaguar and a \$500,000 home without taking out a mortgage. Such tracking would increase security and minimize expensive, time-consuming, full-scale investigations on the five-year reinvestigation cycle.

By using readily available, comprehensive data, the government can shorten processing times dramatically, more effectively allocate vital investigative resources to other cases and have continuous visibility into changes in status for those already cleared.

The private sector long ago mastered these risk management methods, and it is time for the government to catch up and adopt these best practices. The ends are clear and the means are available. Leveraging existing technology, data and analytics are the first steps toward a more efficient process of protecting the nation's classified information and methods. 

John Casciano, senior vice president and CEO of LexisNexis Special Services Inc., is a retired Air Force major general who spent most of his career in intelligence and security.