NEXT STEPS FOR SECURITY REFORM

...Industry Proposals to Enhance Efficiency and Reduce Costs in National Security Contracts...

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

SECURITY CLEARANCE REFORM TASK FORCE

DECEMBER 2011

ACKNOWLEDGEMENTS

INSA CHAIRWOMAN
Frances Fragos Townsend

INSA SENIOR INTELLIGENCE ADVISOR
Charlie Allen

INSA STAFF
Ellen McCarthy, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Jeff Lavine, *INSA Director of Administration and Management*

Ashley Andrews, *INSA Fellow*

Ryan Galluzzo

Emily Gunning

Stephanie Kiel

Kyle Murphy, *INSA Intern*

PARTICIPANTS IN THE SECURITY CLEARANCE REFORM TASK FORCE ***
*Charlie Allen, *INSA; Chertoff Group*

Tony Cothron, *General Dynamics IT*

Linda Dei, *KeyPoint Government Solutions*

Rahul Gupta, *PricewaterhouseCoopers*

Jon Hildebrand, *General Dynamics IT*

Al Krum, *Harris Corporation*

Mitch Lawrence, *AT&T*

Adam Lurie, *USIS*

**Kathy Pherson, *Pherson Associates, LLC*

EDITORIAL REVIEW
Joe Mazzafro

COPY EDITOR
Elizabeth Finan

**Denotes role of Chairman.*

***Denotes role of Vice Chair*

****Participation on the Council does not imply personal or official endorsement of the views in the paper by any participating member or his/her respective parent organization(s).*

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.

EXECUTIVE SUMMARY

Over the past six years, timelines and backlogs in national security clearances have decreased substantially, particularly for government employees. Improvements for private contractors providing specialized services have not been as significant. Policies regarding critical efficiencies such as transportability of clearances and reciprocity between agencies remain an impediment to effective contract management and raise the cost to the American taxpayer for protecting our nation.

> The potential savings from the efficiencies gained could amount to hundreds of millions of dollars.

Inefficiency in government under any circumstances is a source for concern, but it is particularly unacceptable given current efforts to minimize federal spending. Conservative estimates suggest that, at any given point in time, 10 to 20 percent of contractors being paid for by the government are not on the job because of delays associated with security clearances and related policies. These lost man-hours represent billions in taxpayer dollars. Even modest improvements in efficiency could save hundreds of millions of dollars each year.

To address this issue, INSA formed a Security Clearance Reform Task Force, under the leadership of INSA Senior Intelligence Advisor Charlie Allen. Members of this task force share the conviction that the inefficiencies that occur when government contractors try to comply with government security policies can be reduced. The Task Force believes that action should be taken now to conserve resources and to ensure capacity and agility for more critical national security activities. Each member has decades of experience in government service; all are now working in the private sector. Most have worked on security issues for both the government and industry, having served as senior government executives before taking on industrial roles.

The Task Force quickly coalesced on six key issues for continuing security reforms, focusing on those least likely to be apparent from the perspective of government security policy makers and most likely to result in long-term savings. Through interviews with senior government security officials and industrial security experts from small, medium, and large organizations, they validated the problems and shortfalls they observed and formulated options for overcoming them. Members of the Task Force have consistently observed disconnents between the contracting and security processes. Their suggestions have been discussed with senior security officials from across the Intelligence Community (IC) and the Office of the Director of National Intelligence (ODNI).

Improving efficiencies and reaping the benefits will require a meaningful public-private partnership. To that end, our goals for continuing to promote efficiency and improve security practices at reduced costs envision government and industry working together to:

- Track the full costs of contractor security, including high level clearances and secure facility usage, and timeliness of policy implementation and reinvestigations.
- Provide improved security guidelines for use by contracting officials.
- Implement flexible approaches for short-term contractor access to sensitive information.
- Support industry security structures that enable anticipation of government needs and development of solutions and innovations.
- Promote a level playing field across industry for large and small companies.
- Apply security policies clearly and consistently across agencies and companies.

Our discussions focused on a few key drivers that create inefficiencies and obstacles as contractors try to follow security policies while meeting government expectations for quick response. They involve:

- Misapplication of security processes in acquisition.
- Difficulty in moving workers with current access or eligibility across contracts and agencies.
- Confusion between access to national security information and suitability for public trust.
- Inability to access contractor clearance information on a single database equally available to contractors involved in classified government projects.
- Inadequate implementation of available technology and automated identity tools.
- Restrictions on secure facility use across programs.

Our recommendations build on the progress of the past few years, enabling industry to help government maintain a trusted contractor workforce that can accomplish more but cost less. They include specific actions to:

- Align security and contracting processes to minimize cost impacts to both industry and government.
- Make clearance portability a reality, instituting "eligibility in person."
- Complete investigative and suitability standards.
- Spin off a low-side version of Scattered Castles for For Official Use Only clearance data.
- Invest in personnel security automation that has demonstrated reliability and produced savings.
- Allow conversations across programs and contracts, and temporary storage in secure facilities.

THE BOTTOM LINE:

SIX GOALS FOR IMPROVING ACQUISITION SECURITY

This paper builds on INSA's previous report, ***"Improving Security While Managing Risk,"*** published in October 2007, and provides recommendations for more effective contract security management. It takes a strategic view, drawing lessons from the many achievements of the personnel security reform process, and it seeks additional efficiencies and savings that can be realized with a collaborative effort between government and industry. By highlighting the substantial "hidden costs" to the government that result from varying departmental practices for granting security clearances to industry and the lack of standard, integrated, IC-wide management practices and policy approaches, this paper identifies problem areas where costs can be reduced and suggests how to do it.

> 10 to 20% of contractors may not be on the job because of delays associated with security clearances.

We offer the following goals for reforming security policy and practice for industry:

1. Continue improving security processes and metrics for clearances, facilities, policies, and reinvestigations.
2. Decrease costs through implementation of security guidelines that facilitate the agility and responsiveness of cleared and clearable industry personnel.
3. Develop and execute across the IC more flexible approaches to security practices, such as increasing use of "read-in/read-out" access for research, proposal development, or short term projects.
4. Enable industry's capability to anticipate government needs and provide innovative solutions.
5. Promote a level playing field across the full range of industry, large and small.
6. Improve the clear and consistent application of security guidelines across companies and agencies.

At a time of increasing threats and greater resource constraints, improving the contractor security clearance and secure facilities management processes will allow the national security community to keep the country safer and spend fewer taxpayer dollars. Government and industry have a unique responsibility and opportunity to work together to respond to these national security and fiscal imperatives with crosscutting efforts to simplify personnel and facilities security measures.

RECOGNIZING INDUSTRY'S ROLE IN NATIONAL SECURITY

Since 2006, IC leaders and security organizations have made significant progress improving the efficiency of personnel security processes without compromising quality or trust. The focus has been primarily on the processes and practices within and between government organizations. But now that those requirements have been reviewed, validated, and are well into implementation, we have the opportunity to look at the process from the contractor side of the lens, offering perspectives and adjustments to limit unnecessary burdens, avoid duplication or multiplication of effort, and control contractor costs that are fed back to the government in overhead rates. These factors are the source of substantial delays and shortages in mission capacity.

> Now is the time to further refine the process so that industry can deliver more value to government.

Industry is further spurred to offer this collaborative appraisal by several imperatives and initiatives within government.

- Federal budgets for intelligence are shrinking, raising the bar for contractors and government to work together to deliver as much value as possible for scarce acquisition dollars.
- The Government Accountability Office (GAO) has published its review of the improvements to the personnel security process, commending the timeliness of clearance processing but noting a lack of data to assess other security reforms directed by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (see "Appendix A: Clearance Reform in a Nutshell" for more detail).
- The Director of National Intelligence (DNI) Lessons Learned Center seeks to improve the visibility and portability of cost-effective ideas and solutions across agencies.
- An interagency committee continues to work toward finalizing Federal Investigative and Suitability Standards, but completion may be years away.
- President Obama, in the 2011 State of the Union Address, ordered a "review of government regulations," noting that "when we find rules that put an unnecessary burden on businesses, we will fix them."

Notwithstanding the GAO report, key components within security processes may appear to be optimized or resolved from the government's vantage point, but result in specific inefficiencies for contractors and higher costs, reduced agility, and diminished mission capacity for the government. These suboptimizations are often only reported to the government through anecdotes reflecting exceptions to the rule or unforeseen circumstances and not in available data. This situation is not surprising because the metrics were designed to track government progress toward meeting its need for cleared personnel in a timely fashion. That now accomplished, it is the time to further refine the process so that industry can deliver more value to government.

This report focuses on six of the most glaring deficiencies, explains the unintended consequences of poorly targeted security policies, and suggests simple solutions for resolving the inefficiencies without impact to the integrity of security processes. Most are in the personnel security realm, but the reciprocity conundrum spills over into physical security as well. The root causes in each case are traced back to disconnects between the contracting and security processes; the lack of standardization and differing priorities that lead to separate processes; and apparent lack of trust, transparency, and efficiency for contractors who are by and large working across various agencies.

Industrial contractors, critical stakeholders in our national security system, offer perspectives that are not often taken into account in the design of security processes, but are perhaps one of the best ways to test their ability to promptly meet personnel needs without compromising security.

- Contractor success and corporate survival depend on security clearance and access processes that enable the smooth transition and employment of skilled workers and the ability to apply their skills and experience to tasks across the federal workspace.
- Smaller contractors are more sensitive to the impacts of security process changes and can serve as quick feedback mechanisms for positive and negative impacts.
- Contractor reputation and future business depend on their ability to maintain solid security programs that protect their sensitive contracts, allowing them to anticipate, prepare, be eligible, and respond quickly to government requirements while keeping security costs at the lowest possible levels.
- Current contracts, ongoing research, and business development efforts across the IC give contractors visibility into the processes, similarities and differences in implementation, and causes of efficiencies and inefficiencies among the IC's many programs.
- Many security leaders in industry have previously served in senior government security positions and well understand the challenges faced by government and industry.

Today's situation is similar to what drove the creation of the National Industrial Security Program Operating Manual (NISPOM) nearly 20 years ago. Taxpayers need industry to engage again to discuss concrete improvements with government.

MAJOR PROGRESS BUT MORE OPPORTUNITY FOR EFFICIENCY AND COST SAVINGS

Substantial improvements have been made to the personnel security clearance process. Executives in the Office of Management and Budget (OMB), the Office of Personnel Management (OPM), the Office of the Director of National Intelligence (ODNI), and the Department of Defense (DoD) are responsible for these dramatic changes in processing times.The November 2010 GAO report noted "significant overall progress" on personnel security, but lacked data to judge the extent of reciprocity. It recommended continued oversight to sustain momentum.

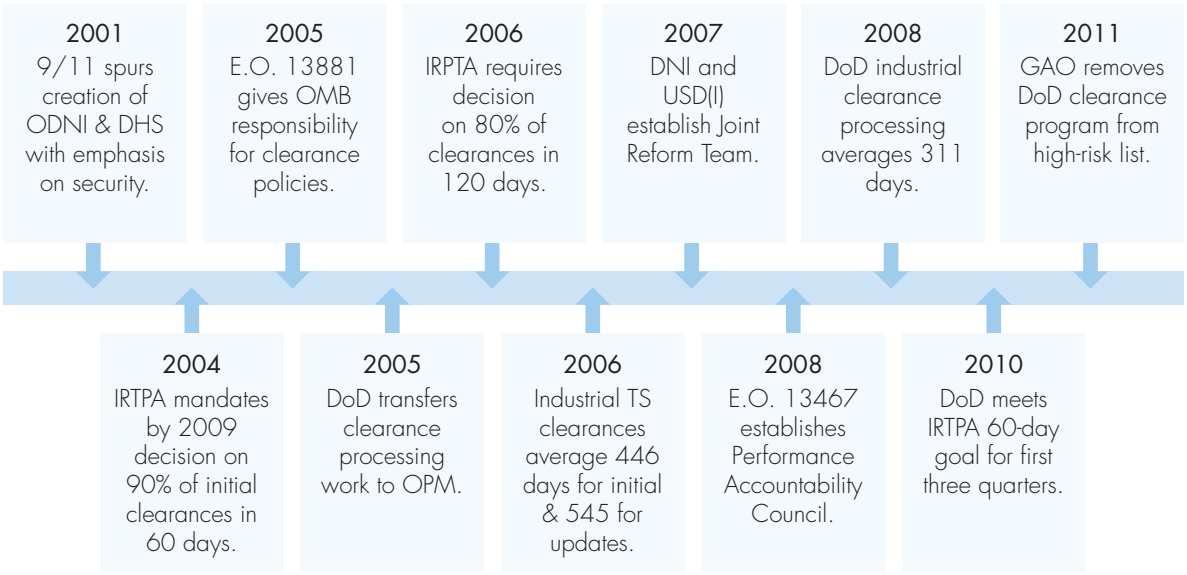

Figure 1: Clearance Improvements since 2001

This white paper validates the GAO assessment and seeks to add data and context not available to the GAO. We believe the best way to sustain momentum is to recognize the costs of industrial security, understand the impact to mission of inefficient and widely varying security practices, and proactively address unnecessary costs and obstacles to improved national security. Initiatives such as E.O. 12829 and the update of the NISPOM in 2006 were critical first steps toward efficiently integrating the contractor community into personnel security clearance policies. We highlight in this report several of the many examples cited by each task force member of security practices that increase costs to the government, decrease mission flexibility and effectiveness, and appear inconsistent with the intent of DNI security policy.

Despite these efforts by government security leaders to improve clearance timeliness and work together as never before to overcome some of the basic problems resulting from lack of standardization, the gains are limited because of the government's tendency to focus primarily on compliance. Industry has been involved in helping the government generate policy improvements, but much more can be done to optimize the policies so they can comply effectively at less cost.

This review concludes that some of the design flaws in the policies result from a misunderstanding or lack of knowledge of real-world contracting and security processes. Current security practices mistakenly assume that:

- Contracts result from discrete, linear, and orderly processes in which:
  - One person works on only one contract.
  - Cleared people will work on contracts and not through purchase orders or other acquisition mechanisms.
  - The Contracting Officer or Contracting Officer's Technical Representative (COTR) know about the contract and are not administering it on behalf of another agency.
  - The contractor's requirement for access will not change quickly, even though the government's needs may change and frequently do.
- One agency is responsible for the contractor's clearance, both owning and updating it. Transfers are not easily built into the system because each agency's implementation systems have vastly different requirements and procedures.

Acquisition Process Changes Lead to Work Stoppage

Exemplifying the unintended consequences resulting from acquisition process alterations, a large contractor was required as part of an "improved process" for an agency it had supported for decades to change the Special Security Office (SSO) servicing its clearances for the contract. For the convenience of the government, the contractor's employee clearances had been held by a military service SSO rather than by the agency it served. When the contractor's security officer asked six months in advance for options to complete the move efficiently, the agency's security officials asserted they could "not transfer in status clearances for contractors" and the contractor's workforce would "have to go through the full security process before being granted a clearance," even though hundreds of the transferees were already working inside the agency or at agency field sites. On the day of the contract change, several hundred contractor personnel whose clearances had not been completed under the new process were denied access and held in the agency auditorium for several hours until a senior agency official granted them waivers to preclude further impact to key mission activities.

- Policies are being carried out consistently by those at operational levels. In practice, the standards are based on judgment, but few contracting officers, technical representatives, or managers are trained in making security policy judgments and have no incentive to understand or relate the impacts of security decisions to contract costs or impacts to their agency or other IC members.
- Short term decisions to meet requirements or risk tolerance for a single contract in one agency have resource impacts on industry and restrict the efficient deployment of contractors to other agencies within the national security system.

The current imperative is to prepare for constrained resources in an increasingly dangerous world. All components of the intelligence and national security communities need to work together to produce savings and stay ahead of the game rather than falling behind as contractors use scarce resources to comply with inadequately-conceived and poorly implemented security policies.

A Clearance Is Government Equity, Not an Industry Commodity

When a cleared worker changes employers–whether industry to industry, government to government, or government to industry–the agency responsible for picking up the clearance at the new employer often cannot easily process the changeover. Recent data from one large contractor reveals an average of 70 days to process clearances for individuals with active TS/SCI clearances moving to a new contract. This even occurs when the worker is moving from one contractor to another within the same agency. Industry's frustration with this "bureaucratic amnesia" is that the government loses sight of the fact that it has paid for and by law owns the clearance, despite which agency or contractor employs the worker.

KEY AREAS FOR IMPROVEMENT

Discussions among several industrial contractors, ranging from very large to very small, and with government security leaders, coalesce around a few processes that appear logical from the government's perspective, but create inefficiencies and obstacles as contractors try to follow the process, anticipate government needs, and strive to meet requirements for timely response. Each has a series of mitigating actions that will have benefits in the short term and will continue to reap efficiencies over the longer term. Many of the actions are simple and could save substantial contractor man-hours that become part of overhead. They involve:

> Government processes should enable the largest possible workforce and encourage qualified contract workers to ensure adequate mission capacity and responsiveness, not limit them unnecessarily or in ways that result in higher costs to the taxpayer.

- Misapplication of security processes in acquisition.
- Difficulty in moving workers with current access or eligibility across contracts and agencies.
- Confusion between access to national security information and suitability for public trust.
- Inability to access contractor clearance information on a single database equally available to contractors involved in classified government projects.
- Inadequate implementation of available technology and automated identity tools.
- Restrictions on SCIF (Sensitive Compartmented Information Facility) use across programs.

1. DISCONNECTS BETWEEN THE ACQUISITION AND SECURITY PROCESSES

A key driver is the lack of synchronization between the critical nodes of the contracting and security processes. Security requirements are written into contracting documents that reflect the letter of the law, but are based on the assumptions of a long-outdated hierarchical model. The reality is that companies, even small ones, work for multiple agencies requiring Top Secret clearances and compartments. Furthermore, cleared employees rarely work on a single classified contract.

Inefficient Processes Spur Cottage Industries and Raise Government Costs

Hiring pressures resulting from the current clearance system have created a cottage industry for locating and recruiting cleared workers for government contractors and agencies. One website, clearedpeople.com, owes its existence to government contract requirements for staffing cleared people at the time of contract award, as well as many agencies' failure to allow companies to have "bench strength." Companies are being created to handle the transfer of large numbers of cleared staff from one company to another as a result of the loss of a contract, such as when Boeing wins a large contract from Lockheed or vice versa. Contract background investigator companies, a rarity fifteen years ago, are now ubiquitous in the government's clearance programs. Bottom line: When the government hinders or cannot provide a service, entrepreneurs gain opportunities to profit legally from the inefficiencies. Whether the immediate costs are covered by the government or the contractor, the taxpayers eventually pay the bill whether they know it or not.

Even though initial clearances are processed faster and contract resources are tighter, the demand for experienced, cleared workers continues to be high. Companies must leverage the expertise of highly skilled and cleared workers across multiple programs to develop and propose needed technical and manpower solutions, spread the cost of greater expertise, and facilitate a broader range of beneficial impacts for government clients. Many of these workers have additional value based on their experience solving complex problems as senior government officials.

Industry Pre-Screening Saves Time and Money

Industrial pre-screening weeds out a credible number of persons who may not make it through the clearance process so that the government does not have to do the same with taxpayer money. Although there is no national policy mandating the use of pre-screening, virtually every company already conducts pre-screens as part of its own due diligence hiring practices. These pre-screens usually include drug screening, personal interviews, credit checks, and police checks—most of the elements of a background investigation. Companies, if they want to stay in business, are just as interested as the government—albeit for different reasons—in making sure they hire honest, loyal, and law-abiding citizens.

Competition among federal contractors is always fierce, but it is becoming even more so as contract budgets shrink and government requirements remain just as pressing. Contractual Requests for Proposal (RFP) that stipulate bidding only cleared workers—or workers with a specific agency clearance—force contractors to pre-position personnel on existing contracts so they can be bid on forthcoming projects.

This situation is further complicated by the pressure from Congress and other overseers to keep numbers of cleared employees to a minimum. This restraining force hampers companies' ability to maintain cleared and qualified staffs to carry out the corporate administrative, information technology, business development, research, and security functions required by the government. What results is an industry scramble to rejustify or find new contracts to cover support clearances when agencies periodically scrub contract clearances. With no IC-wide policy approach to the administrative and business security clearance and facility needs of industry, individual contracting and technical representatives have become the arbitrary limiting factors for access.

To be successful, contractors must anticipate government needs, preparing to propose solutions in many cases before the government has articulated the problem, held an industry day, or disseminated an RFP. Without a bench of cleared personnel and appropriately cleared facilities, companies are at a disadvantage—or, depending on the wording in the RFP, may not even be eligible—for contracting opportunities.

For instance:

- RFPs that require proposed contractor staff to hold current clearances at a specific agency by definition rule out those who are eligible for immediate crossover. This stipulation is intended by the contracting officers to enable a rapid start to the project, but security officials confirm that crossovers for eligible personnel are quickly processed, often in hours.
- RFPs that call for "accredited Sensitive Compartmented Information Facilities (SCIFs)" by definition mean that the facility is not just appropriately constructed, but that it is already in use for another contract for the same agency. Again intended to minimize start-up complications, this also limits the competition to companies that have current contracts with the organization.

Reasonable rates depend on keeping overhead—or non-billable contract-related costs—to a minimum. Government contracting processes that encourage pre-positioning cleared workers disadvantage small companies without large overhead cost pools, raise overhead costs for all companies that are charged back to the government in higher labor rates, and reduce the productivity of cleared workers on hold pending contract awards and work initiation. This vicious cycle makes it even more difficult for new businesses to compete successfully for opportunities without an established partner or a lucky break.

Industry is taking increasing responsibility to ensure the security of its contracts and making sure its employees' investigations are current. Several major defense contractors and other consultants have instituted facsimiles of the government's clearance processes as part of their conditional hiring, consolidated personnel security processes at a corporate level, and are collaborating with one another on best practices for saving resources without sacrificing quality.

Looking at the problem from both the contractor or compliance perspective and the government or regulatory viewpoint avoids one-sided solutions that miss needed improvements to the overall process. Historically we have focused on establishing priorities for applying established clearance processes rather than seeking to maximize the government's trust in available resources. This results in shifting priorities among staff/contractors and initial clearances/reinvestigations, differing agency capabilities and processes, and disconnects between security and acquisition.

Contractor security officials note that the problem is often not the security process, but the application of security policy and regulations by contracts officers. The two need to work together to ensure the entire process fits reality. Government processes should enable the largest possible workforce and encourage qualified contract workers to ensure adequate mission capacity and responsiveness, not limit them unnecessarily or in ways that result in higher costs to the taxpayer.

Contractors Face Difficulty in Moving to New Contracts if Reinvestigation Due

IRTPA mandated that most initial security clearances be granted within 60 days, without establishing a similar requirement for periodic reinvestigations. Many contract personnel work on a variety of contracts over the course of the five years between periodic reinvestigations, and frequently face difficulties with their clearances if they must transfer across projects and agencies around the five-year mark. However, without measuring and mandating improvements in reinvestigation timeliness, policymakers lack the data that would expose this as a problem or generate understanding that policy gaps have created unnecessary costs.

2. CLEARANCE AND REINVESTIGATION RECIPROCITY AND PORTABILITY

The security community has worked hard to make reciprocity a reality, but it remains a concept that is often expressed in word, but not consistently in deed. Part of the problem is definitional: what is referred to as "reciprocity" supports "crossover" or what is more accurately called "clearance portability." Movement of individuals with appropriate accesses should be transparent and quick so that industry can:

- Reduce cost and improve responsiveness to government needs.
- Meet government mission requirements efficiently and quickly.
- Maintain agility and therefore competitiveness in the federal marketplace.
- Support monitoring of employees for trustworthiness and timely reinvestigation or maintenance of "scope" across agencies.

Delays in portability persist despite revisions in government policies and standards because each agency implements security procedures idiosyncratically with little or no consideration for connections to or best practices by other members of the community. Intelligence agencies have standardized processes within their particular agency, but most are designed independently from related processes in other agencies. Within the Department of Defense, for example, some contractors have documented over 300 separate personnel security processes required by the Air Force, Navy, and Marine Corps.

To government agencies, this inefficiency is simply the "cost of doing business" and establishes commonality within their stovepipe, but the cost to the contractor is substantial—and sometimes disastrous—in lost productivity, unmet deadlines, and maintaining workers on overhead. We estimate that some 10 to 20 percent of the personnel required and contracted by IC agencies are not on the job because of security delays. Much of the inefficiency could be remediated with streamlined agency processes that accept active, cleared people as "eligible" to begin work on any classified project with minimal processing. Those with clearance histories or working across multiple agencies—with "eligibility in person"—should be rapidly transitioned across contracts and agencies, helping to spread best practices and encourage collaboration and community.

Costs of contractor redeployment can be large even within a single agency. In many agencies, a contract employee with active clearances must complete the entire security administrative process and resubmit forms when moving from one program to another or when added to a new program. Likewise, a contractor changing companies on the same contract must submit the entire package for approval. Efficiencies should not take a back seat to traditional practices unsupported by data proving the benefits are worth the cost, particularly as budget restrictions lead to tighter contract margins.

Part of the problem stems from the experience of individual security officers, their ability to evaluate situations that do not fit the standard or the checklist, and the inconsistent interpretation and application of policies and processes across agencies. The lack of experience, management, and critical thinking at the third or fourth echelons leads to risk avoidance based on fear of doing something wrong, unsophisticated knowledge of the standards, and a "checklist mentality" that substitutes for analytically solid judgments about protecting what is really sensitive. Since the real cost is not visible to the government, the end result is much higher costs, decreased capacity, and reduced responsiveness by industry for the IC.

The disconnects among agency security processes for those who hold clearances in multiple agencies play out in a number of other ways that impact both resources and compliance. One easily resolvable process involves travel, foreign contacts, and outside activity reports that clearance holders are required to submit. Each agency has its own reporting and approval process, often requiring the individual to submit a form on internal information systems, even though not all cleared contractors work on site or require access to the system. The Industrial Security Working Group (ISWG), a self-organized consortium of contractor security representatives, in 2006 devised a common form that met community standards and could be submitted in hard copy. Most community agencies refused to accept the initiative. The result is a confusing set of individual agency travel processes that adds costs for industry personnel working on and among multiple contracts.

No Excuse for Crossover Delays for Cleared Contractors

Despite metrics on reduced cycle times and assertions by security managers that crossovers are accomplished in hours or days, contractors frequently cite experiences in which skilled workers with long-time clearances inexplicably wait weeks to be processed to work on a contract in another agency. For instance, one agency's retiree with contractor accesses in two different IC organizations waited four weeks to be crossed over for an IC program in early 2011. Delays in clearance transfers transcend rank or seniority; former admirals or senior congressional staffers can be delayed just as long or longer as mid-level managers or entry-level staffers. Anecdotes do not replace metrics, but they provide the "use cases" or indicators of process flaws that might easily be monitored or highlighted for improvement.

Even more disquieting are the unintended results from variations in agency processes for contractor clearance reinvestigations, which can have real impact on a company's competitive prospects. Some agencies are keeping up with the five-year reinvestigative scope standard and even more stringently specifying that anyone in their system be in scope. Others, in tacit acknowledgement that the five-year reinvestigation period is an arbitrary standard with no clear evidential connection to maintenance of public trust, have opted to postpone reinvestigations in an effort to apply shrinking resources to more critical purposes. This may make sense from a specific agency's point of view and resource allocation, but it hampers the movement of cleared contractors to do the government's business and so becomes a short-term decision with long-term impact.

Today, community security leaders do not have a way to measure unmet reinvestigation demands. IRTPA does not mandate a measure of reinvestigations, but agencies could be required to report on clearance reinvestigations they never undertake and justify their decisions. Evolving methodologies and databases that facilitate continuous evaluation, periodic partial reinvestigations, and involved managers also can help mitigate longer times between investigations, if resources are a problem. What does not work is to have one agency decide to forgo investigations, thereby shifting the responsibility and cost for reinvestigation to another agency at potentially greater cost because it lacks the historical clearance files.

Inefficiency could be remediated with streamlined agency processes that accept active, cleared people as "eligible" to begin work on any classified project with minimal processing.

Restricting the Number of Clearances Does Not Always Save Money

Some agencies will not allow indirect labor, such as senior company executives, contract managers, recruiters, business developers and even security staff, to be granted clearances to work on contracts they have been awarded. A number of poorly thought out reasons are given for these decisions, including:

- *They do not work directly on the contract.* The reality is that identifying the functions as direct labor would only drive up contract costs; thus they are submitted as indirect labor and not allowed to bill to the contract.
- *Having more people cleared will cost the government more money to clear them.* The hidden costs of protecting and "interpreting" the cleared contract for uncleared support personnel raises the potential for security incidents and unintentional disclosures by people who did not know they were working with unclassified but potentially sensitive information. It also leaves open the possibility of proliferation of parsed classified information that has to be given for compliance with government regulations, such as Sarbanes-Oxley, Defense Contract Audit Agency (DCAA) auditing, Federal Acquisition Regulation (FAR), and Defense Federal Acquisition Regulation Supplement (DFARS).
- *Clearing support personnel will add to the company's overhead rate, which will be passed on to the government in higher rates.* They are already overhead, whether they have a clearance or not.

One agency informed a company's support personnel that they should use their clearances with another agency to work on the first agency's classified contracts. The government contracts officer would only allow technically-skilled workers to be cleared on its agency's efforts and disallowed clearances for any non-technical worker.

Industry and government should be working together to continue driving down the costs of investigations and reinvestigations. The large contractors who are taking on the responsibility to incorporate background investigations that meet government standards into their hiring practices are doing so to expedite cycle times and conserve resources. To take full advantage of industry's efforts to police itself, the government needs to enhance the clarity of adjudicative standards and criteria so industry can understand what it is looking for and pre-screen accordingly. While full standardization is probably not a realistic goal, at least agency tolerance for risk can be more clearly articulated.

The bottom line is that government security agencies would benefit the taxpayer, industry, and the community if they worked together on implementation efforts. This is a problem that frustrates cross-agency programs, but can be deadly for industrial contractors who must complete the same processes in multiple ways. For example, after the Standard Form [SF]-86 is completed, organizational processes run the gamut from paper and manual processes to OPM's automated Electronic Questionnaires for Investigations Processing (eQIP). With paperwork, mistakes are made and the paperwork comes back to be reworked. We can do this more simply and reliably.

Poor Coordination Results in Job Loss for Military in Transition

Active duty and reserve military should have easy transitions to continued government service as cleared contractors. This is an efficiency win-win for the government and industry. Glitches in or between clearance systems cause delays that ultimately force contractors to let go of those transitioning from military service whose clearances should have been easily transferred. For instance, a company processing an active reservist recently had to let her go because delays in processing her clearance precluded getting her on the job to cover her salary and benefits. One of her reserve unit security specialists expressed frustration that a job was lost because no one thought to have the reserve unit cross her clearance directly to the company through the Joint Personnel Access System (JPAS). Another former military officer lost his job in June 2011 because his company could not figure out how to rectify a system overreaction resulting from a one-time late mortgage payment. He gained another job at a smaller company that researched the situation and realized that his clearances had been active all along.

3. FEDERAL INVESTIGATIVE STANDARDS AND SUITABILITY

Improvements in initial clearance timeliness have been of little benefit to industrial contractors who are subject to separate and additional suitability adjudications. In some cases, highly skilled and in-demand contractors who have been cleared to the most sensitive national security information for decades have been delayed for months pending suitability reviews. Furthermore, the criteria and thresholds for suitability decisions and the processes are opaque, so there is little that can be done to prepare or pre-screen for the process.

This problem is specific to a few federal departments, but bears mention in this review because the processes are so inefficient, and the cost to the contractor and the government client overhead costs and lost productivity have been severe. According to government security officials, department and agency heads have full control over their personnel profiles. They warn against blaming clearance processes rather than the unique implementation of suitability standards by a single agency.

The lack of standardization in investigative and suitability standards has been a goal of the Joint Reform Task Force since 2008. The change and delays in issuing the Federal Investigative Standards do not help. According to our most recent information, the standards may not be fully implemented for two more years.

Part of the confusion is that the difference between security and suitability is not just misunderstood, but misapplied. Industrial contractors or government employees whose jobs require access to national security information and do not carry out law enforcement responsibilities should not go through both processes. The five tiers in the current set of standards represent an effort to distinguish more clearly between the two concepts. More work needs to be done on building a solid conceptual framework for federal trust; this may well be addressed in a planned study by the President's Intelligence Advisory Board.

Training and collaboration are essential. The Defense Security Service (DSS) reportedly is developing a course on suitability. While it should be commended for taking the initiative, the IC may well have to develop a separate suitability course if cross-agency agreement is not reached on foreign investigative standards. This is further complicated by differing schedules and means in implementing Homeland Security Presidential Directive 12 on employee and contractor identification standards. In any event, security officers need to be trained to deal with policy exceptions, not just checklists and compliance systems. They should be familiar with appropriate means for challenging or finding acceptable alternatives for policies that might not apply. This is another area in which collaboration and community must be emphasized for the benefit of the nation and the taxpayer.

4. CLEARANCE DATABASE

This review reaffirms the need for a database accessible at an unclassified, but controlled, level that holds basic clearance information for rapid determination of "eligibility in person" of skilled and cleared assets to meet government requirements expeditiously. The Department of Defense's JPAS currently serves this purpose, providing clearance data and visit certifications; however, it has become a service of "common concern" because although it is available, it is aging and neither intuitive nor user-friendly.

Some government agencies will not populate the clearance databases even when not doing so prevents individuals from applying their expertise to other government projects.

The DNI's Scattered Castles database is only available to those industrial contractors who have access to classified systems. Even when data from Scattered Castles is required in contract proposals, not all government security offices will provide the information to industrial contractors. This is particularly a complication for small business since failure to accurately fill in all the blanks can be used as a rationale for judging the entire proposal to be non-compliant and therefore non-competitive.

Some agencies confuse contractors' need for access to clearance data with a demand that all clearances be contained in a single unclassified database. One non-Defense agency even has a policy disallowing its employee data on JPAS despite inclusion of many current and former employees working with Defense agencies. A clearance database on a secure network that is not available to all industrial contractors doing classified work is not the solution, even if it contains nearly all cleared personnel. Contractors responding to RFPs that require clearance data in unclassified or For Official Use Only (FOUO) formats should have equal means to access the data. Like JPAS, such a database does not have to contain sponsor information and certainly does not need to contain sensitive names.

We were surprised to learn that some government agencies will not populate the clearance databases even when not doing so prevents individuals from applying their expertise to other government projects. One industry contractor recently complained about the refusal of security officials at OPM and the U.S. Congress to enter data in JPAS to facilitate the process for an employee transitioning to a contract status to support senior officers in another agency. The response "we don't do that" is unacceptable when cleared, experienced people can contribute to solutions for other government organizations.

In the short-term, synchronizing the data across the two systems and making it available on either system can significantly increase the return on the government's investment in people. Scattered Castles already uploads JPAS data, but an effort should be made to filter basic clearance data for non-covert personnel to JPAS or a low-side Scattered Castles "Lite." Over the longer-term, current initiatives in developing Scattered Castles promise multiple ways to resolve this at reasonable cost.

5. APPLYING TECHNOLOGY TO IMPROVE SECURITY PROCESSES

Community security leaders also have made significant strides in the use of and commitment to technology. The Security and Suitability Process Reform Strategic Framework for February 2010 provides a clear focus and specific objectives on using technology to improve security. Government systems such as OPM's eQIP and the Army's Case Adjudication Tracking System (CATS) have begun to infuse technology and automation into a process that has been inherently manual.

Many opportunities exist for the government to continue injecting modern technological methods to enhance the clearance process, focusing on the need for processing expediency, investigative accuracy, fiscal responsibility, and clearance reciprocity. None of these concepts is new, but each deserves continued consideration even in times of resource constraints. Government security organizations have demonstrated a long-term discomfort in how much technology to adopt; opportunities have been lost during abundant resource environments and will not be any easier now.

End to End Case Management.

The February 2010 Joint Reform Team (JRT) yearly report noted that "end to end automation" of the personnel security clearance process is still an underlying goal of the reform effort and an enterprise structure is still required to "manage and monitor cases and maintain relevant documentation of the security or suitability application, investigation, adjudication, and continuous evaluation processes." During the JRT's review, the structure of the security clearance workflow highlighted seven "operational modules" that are being carried out by most government agencies, even if not in the same way:

1. Need Validation
2. eApplication
3. Automated Records Check
4. eAdjudication
5. Enhanced Subject Interview
6. Expandable Focused Investigation
7. Continuous Evaluation

An End to End Case Management System could help bring uniformity, commonality, and consistency to personnel security processes across the government. It could improve the timeliness and visibility of personnel security data by connecting current standard commercial and government systems, providing process transparency to all engaged in enterprise management, and expeditiously moving data through each touch point in the process. For example, maintaining a tracking record of the needs validation throughout the individual's clearance process would prevent other agencies from initiating duplicative clearances processes. Overcoming the obstacles of visibility and transparency into personnel security process data across agencies can reduce duplicative efforts that increase cycle times and costs.

Electronic records management processes would allow agencies to speed up requests and transfers, dramatically improving reciprocity and the portability of clearances.

Digital Fingerprint Collection.

Digitally processed fingerprints can be submitted to the FBI electronically with a fraction of the error rates of ink and paper prints. They result in turnaround times that are less than two days, rather than a month with paper prints sent to the Bureau through the U.S. mail. Additional benefits of electronic submission include enhanced quality control of the data, easier integration into the electronic workflow process, and reduced probability for identity fraud. The data can be consistently maintained through entire clearance history, resulting in long term savings and overcoming stovepipes.

Electronic Records Management.

At the completion of the security clearance process, most agencies store the information from the investigative process in hard copy files that must be copied or physically transferred to be shared. Electronic records management processes would allow agencies to speed up requests and data or file transfers, dramatically improving reciprocity and the portability of clearances. An IC, enterprise-wide electronically managed personnel security system would improve overall security, enable risk management, drive down costs of clearances, and, most importantly, improve the "time to job" of getting government and industry personnel cleared and at their new task.

Interactive Investigative Tools.

Few agencies have taken advantage of the significant technology tools currently in the marketplace that could improve processes. For instance, rather than taking interview reports with pen and paper, electronic pens that transcribe handwriting into an electronic report could reduce the time spent writing reports. The templates could be uploaded to a centralized system, limiting recontacts to those subjects or sources later on.

Performance-based Scheduling.

With a vast network and dramatically fragmented population of government and industry personnel working in the personnel clearance system, an automated scheduling system designed to allocate work based on performance could improve efficiencies by limiting the human element in work scheduling. The Army's electronic adjudication system, CATS, has demonstrated positive results using a similar function.

Internet and Social Media Use.

The personnel security community lacks a policy allowing the effective use of the Internet or publicly available social media data during the risk mitigation process. Federal agencies should be allowed to follow common industry practice and use information posted publicly on the Internet during the investigation process. This growing information source will immediately bring added qualitative value to the data gathering process.

6. SECURE FACILITIES

The goal of Intelligence Community Directive 705 and the recently released Technical Standards for SCIFs is to codify the intent of the IC that SCIFs should be reciprocal. Portability of SCIFs across contracts and agencies should help contractors manage the costs and enable more efficient use of secure space to support the government. However, each agency is responsible for developing its own implementation processes, which will inevitably result in differing requirements, costs, and perhaps even timelines. Furthermore, the new policies do not alleviate the problem that companies, particularly small ones, have in acquiring and maintaining SCIF space to pursue new contracts if they do not already have agency-approved SCIF space.

The ODNI as the security executive agent must continue to evaluate the specific impacts the new standards and directives will have on contractor planning and program implementation.

We applaud the establishment of a single SCIF "build to" standard and mandate of a reciprocal use standard, but are concerned that:

- The role of the Certified Tempest Technical Authority and required pre-approvals will hamper contractors' abilities to take advantage of cost-effective space in anticipation of government requirements.
- Conversion of certified space from support for one agency to another is not addressed.
- Requirements for approvals for discussion of one agency's classified information in another agency's classified space, even when all are cleared to the appropriate level, are not alleviated.
- Getting space approved in a timely manner to support pre-contract award activities is dependent on an outside agency that has no vested interest in timely action.

To ensure meaningful implementation, the ODNI as the security executive agent must continue to evaluate the specific impacts the new standards and directives will have on contractor planning and program implementation, highlighting efficient best practices and inconsistencies among various government agency requirements and processes.

RECOMMENDATIONS

Our suggestions are geared toward industry helping government maximize protection for national security programs and information, and building on the progress of the past several years to improve the maintenance of a trusted contractor workforce that can accomplish more but cost less. For the most part, the solutions require leadership and awareness of the impact of policies at all levels; the potential savings from the efficiencies gained could amount to hundreds of millions of dollars. While improved technology can reap huge benefits in terms of data accountability, process consistency, and timeline reductions, the costs may be prohibitive in this budget climate. Any initiatives should have realistic plans for savings over the long term with specific savings targets since we lack data for the true cost of industrial security.

1. ALIGN SECURITY AND CONTRACTING PROCESSES TO MINIMIZE COST IMPACTS TO INDUSTRY AND GOVERNMENT.

- Continue consistent and visible leadership on security clearance issues.
- Reenergize efforts to instill a Community mindset about security processes, looking for opportunities to standardize and simplify processes and practices.
- Develop security implementation policy guidance for contracting officers and contract technical representatives and a mechanism for industry reporting of perceived contracting security decisions that do not support ODNI objectives for effective and efficient industry security.
- Update E.O. 12829 to formalize the NISPPAC's role in addressing current contractor clearance issues.
- Bring the NISPOM into compliance with recommendations as they are implemented.

2. MAKE CLEARANCE PORTABILITY A REALITY.

- Institute "eligibility in person," disconnecting the clearance from the contract and connecting the access to the contract.
- Solve the standardization problem across agencies by accepting the contractors' eligibility for access, then performing any additional processing on the "other side."
- Accept use of a common hardcopy mechanism for reporting travel, activities, and publications for those who do not require access to information systems with information regarding the process on an easily accessible website.
- Require agencies to report metrics on eligibility acceptances and reinvestigations not begun. One way to do this could be through Congressional action to expand IRTPA reporting to include data on clearance reinvestigations and contractor clearance portability delays. The delays are real costs not just to the contractor, but to the government and the taxpayers.
- Increase use of "read-in/read-out" clearances for research, proposal development, or short term projects.
- Allow clearances for contractors who are anticipating government requirements and working on potential solutions before contract RFPs are completed.
- Encourage industry use of consistent pre-screening forms and processes.
- Institute an IC mechanism to collect anecdotes regarding reciprocity failures.
- Train contracts officers and adjudicators in making decisions based on analytic thinking, using checklists appropriately, and dealing with exceptions to policies and standards.
- Reevaluate the basis for the five-year reinvestigation standard and less costly alternatives, including continuous evaluation and random investigation.

3. COMPLETE INVESTIGATIVE AND SUITABILITY STANDARDS.

- Press for the issuance of Federal Investigative Standards that are long overdue.
- Decouple suitability requirements for contractors who only require access to national security information.

The solutions require leadership and awareness of the impact of policies at all levels.

4. SPIN OFF A LOW-SIDE VERSION OF SCATTERED CASTLES FOR FOUO CLEARANCE DATA.

- Filter data from Scattered Castles into JPAS or a low-side Scattered Castles "Lite" to hold clearance data required for proposals and visit for overt personnel without identification of sponsors.
- Ensure low-side clearance databases are equally available to contractors required to track and submit security clearance data for contract proposal and execution.

5. INVEST IN PERSONNEL SECURITY AUTOMATION THAT HAS DEMONSTRATED RELIABILITY AND PRODUCED SAVINGS.

- Continue to seek ways to streamline and improve personnel security processes and databases through infusion of cost-effective technological tools and solutions.
- Encourage use of e-forms like eQIP and other efficient ways to update personal information.

6. ALLOW CONVERSATIONS ACROSS PROGRAMS AND CONTRACTS, AND TEMPORARY STORAGE IN SECURE FACILITIES.

- Enact policy to ensure that an industry SCIF certified to IC SCIF standards with no waivers should be available for use in support of any other agency, project, discussion, or planning activity consistent with cost accounting standards and any special security constraints.
- Reconsider ICD 705 stipulation that SCIFs must have pre-established sponsorship and eliminate RFPs that call for already accredited SCIFs.
- Require agencies to report metrics on implementation of revised standards to determine if they have the desired effect of cross-programmatic utility and efficiency.

WORKING TOGETHER FOR CONTINUED REFORM

While additional efficiencies are achievable, the government deserves great credit for the progress that has been made. Security clearance processing is only one part of a very complex security system. Protecting our national security information is critical, but doing so in a manner that is reasonable, employs risk management processes, and enables the most efficient use of personnel–government and contractor–in whom the taxpayer has invested, is equally critical. Security policy and practice must enable efficient use of limited government resources, not impede efficiency. The current web of security policies and disconnected implementation across government agencies is far from optimized to achieve that goal.

This review is intended to energize the discourse on security policy and its implementation to achieve a security framework that fully enables efficient cooperation and collaboration between the government and industrial contractor communities and minimizes costs to U.S. taxpayers. Over the coming months, we will forge an effective public-private partnership by:

- Initiating discussions with the DNI, agency leaders, and interested Congressional staff.
- Fleshing out ideas for rapid progress on the six key issues by designing solutions with all stakeholders in mind.
- Developing concepts for data collection and analysis mechanisms to provide the DNI and Congress with aggregate data on contractor costs to implement security, savings and impacts as changes are implemented. This data will provide insight on the implications of changes on small business.

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

APPENDIX A:

CLEARANCE REFORM IN A NUTSHELL

In the wake of the 9/11 attacks, Congress sought to reorganize and reform our intelligence apparatus by enacting the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The Act's Title III mandated:

- Adjudication of 90 percent of all initial clearance applications within 60 days.
- Selection of a single executive agency or department to oversee government-wide personnel security clearances and lead a reform effort to dramatically improve their processing and management. Among the assignments given to the selected agency in Title III were developing uniform policies and procedures to determine eligibility for access to classified information, ensuring timely completion of clearance investigations and adjudications, and establishing reciprocal recognition of access to classified information across government agencies.

As a result, initial top secret security clearance processing that was taking as long as 400 days is now typically completed in a fraction of that time. After years of negative assessments, the Government Accountability Office's report in 2010 celebrated the major improvements that had been made, recommended continued oversight to sustain momentum, and identified the need to further investigate the extent of clearance reciprocity across the community. This extraordinary accomplishment was achieved due particularly to the diligence and innovation of the Office of the Director of National Intelligence, the Office of Management and Budget, the Office of Personnel Management, and the Department of Defense.

In 2008, President George W. Bush brought these organizations together as the Joint Suitability and Security Clearance Reform Team (Joint Reform Team, or JRT) to produce an initial proposal for comprehensive reform. Their Security and Suitability Process Reform Initial Report provided the basis for Executive Order (E.O.) 13467, which:

- Created a Performance Accountability Council (PAC) to ensure the alignment of suitability and security processes and to monitor the reform effort's progress.
- Named the Director of National Intelligence as the Security Executive Agent—the new government-wide overseer of personnel security clearances.
- Provided a list of key reform objectives, including:
  - Creating consistent standards for suitability, contractor fitness, and eligibility for access to classified information.
  - Ensuring that consistent standards translate into clearance reciprocity across agencies.
  - Integrating information technology and other innovations to make clearance processing and management more secure and efficient.

Efforts to improve personnel security processing to protect national security began long before E.O. 13467 and IRTPA, stretching back to the commission headed by General Richard Stilwell that reviewed Defense security and policies in 1985 in the wake of the Walker spy case. E.O. 12829, signed in early 1993, established the National Industrial Security Program (NISP) to protect classified information that is released to contractors by controlling means of release, facilities, and the personnel security clearance issues that go along with both. E.O. 12829 calls on the NISP to "serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests." The order also created the National Industrial Security Program Policy Advisory Committee (NISPPAC) and called for the issuance of a National Industrial Security Program Operating Manual (NISPOM). In 2006, the NISPOM was reissued with many updates to the section on facilities and personnel security clearances.

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 160 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
SUPPORTING ADVANCES IN THE NATIONAL SECURITY AGENDA

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org