SECURITY CLEARANCE RECIPROCITY: Obstacles and Opportunities

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
Security Policy Reform Council

June 2019

INSA SECURITY POLICY REFORM COUNCIL

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to develop this report.

INSA MEMBERS

Mary Edington, *KPMG*

Jeremy Erb, *Deloitte*

Laurel Pearson Lloyd, *Peraton*

Kathy Pherson, *Pherson Associates*

Gregory Torres, *Booz Allen Hamilton*

INSA STAFF

Chuck Alsup, *President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director, Communications and Policy*

Ehrl Alba, *Digital Marketing Manager*

EXECUTIVE SUMMARY

The movement of personnel with a security clearance across employers, federal contracts, and the Federal Government, is a common practice. However, government agencies' policies, practices, and resource allocations impede the ability to move cleared federal contractors and federal employees from one agency to another, a practice primarily referred to as reciprocity. Delays caused by misinterpretation of policies and bureaucratic inefficiencies prevent cleared contractors from effectively executing their contracts and deprive the government of labor needed to advance critical national security missions.

Reciprocity delays also result in unnecessary overhead costs for contractors that translate into higher contract rates. Although it is hard to quantify the impact, a rough calculation suggests that delays caused by administrative inefficiencies result each year in the loss of 1,000 contractor labor-years with a total value of $2 billion in the Intelligence Community alone. The cost to the federal government as a whole could approach 90,000 lost contractor labor-years valued at more than $8 billion. Adding the value of federal employees' lost productivity would drive these figures even higher.

The end result is that because of the delays in the investigation and adjudication processes, as well as the systemic delays surrounding reciprocity, the Federal Government is missing out on access to talent, and the national security mission is suffering. By law and IC policy, the Director of National Intelligence (DNI) and the directors of individual agencies have a responsibility to clarify the intent behind policies and fix process inefficiencies. If they do so, the Intelligence Community, the Defense Department, and the U.S. taxpayer will see improved government effectiveness, enormous cost savings, and enhanced national security impact.

Reciprocity delays affect both government employees and cleared contractors. When government employees undertake rotational assignments, their clearances must be transferred from their home agencies and certified by the receiving agencies, which may require additional information to be gathered or updated before granting the employee access to facilities and computer networks. Contractors regularly support multiple agencies, and must transfer their clearances more frequently than government employees. This paper thus focuses principally on the impact of reciprocity delays on contractors.

> Because of the delays in the investigation and adjudication processes, as well as the systemic delays surrounding reciprocity, the Federal Government is missing out on access to talent, and the national security mission is suffering.

Three principal categories of impediments drive reciprocity delays and costs:

AMBIGUOUS OR MISINTERPRETATION OF POLICY

- Many agencies have security policies and procedures that appear to be inconsistent with national-level policy, adding redundant requirements and time delays to clearance transfer requests for both government employees and contractors.
- Some intelligence agencies consider an in-progress reinvestigation (including a completed but unadjudicated reinvestigation) to be sufficient to deny reciprocity for currently eligible and cleared personnel, even if no derogatory information exists.
- Some agencies adjudicate the same investigation twice to the same standard – first for Top Secret (TS) access, then for access to Sensitive Compartmented Information (SCI) soon afterwards.
- The government limits industry access to the official system of record (the Intelligence Community's Scattered Castles database), which industry is required to use to meet contractual requirements, causing delays in clearance validation.
- The November 2018 Security Executive Agent Directive (SEAD) 7 on Reciprocity provides too much room for interpretation by agencies and is silent on previous policies that are no longer required.

LIMITED INFORMATION-SHARING AMONG AGENCIES

- Agencies process exception cases – instances in which a person is granted eligibility by another agency where issues of potential concern were mitigated or under certain conditions (such as ongoing monitoring) – by ordering a copy of the original investigation, which can take months to obtain and re-adjudicate because many are printed in hard copy and mailed.[1]

RESOURCE PRIORITIZATION AND ALLOCATION

- Timeliness standards for investigation and adjudication exclude time required to conduct and adjudicate polygraph exams. While this process is often completed in several weeks or months, it has caused delays of as much as 12 to 18 months before an agency accepts a contractor who already holds a TS/SCI clearance.

[1] *"Personnel Security Exception" is defined in full in Intelligence Community Standard (ICS) 700-1 (April 4, 2008), pp. 17-18. As of February 20, 2018: https://fas.org/irp/dni/icd/ics-700-1.pdf.*

RECOMMENDATIONS

INSA recommends that the Director of National Intelligence (DNI), as the government's Security Executive Agent (SecEA), work with agencies across the Federal Government to take 14 specific steps (listed in the final section of the paper) that would mitigate policy ambiguities or misinterpretations and inconsistent practice across government. Together, these policy and procedural recommendations would:

- Identify practical impediments to efficient reciprocal recognition of clearances and direct agencies to remove such impediments;
- Use available technology to increase the speed at which reciprocity decisions can be made;
- Resource all government adjudication and polygraph staffs to levels needed to meet appropriate timeliness goals, including on-boarding of currently cleared personnel within 30 days;
- Enable currently cleared contractors and government employees to begin work at a new agency while additional information is collected and adjudicated;
- Prevent the adjudication of individuals to the same standard twice;
- Require greater information-sharing regarding personnel clearances among and between government agencies and their industry partners, as a lack of transparency prevents security officers from trusting other agencies' clearance decisions; and
- Enable contractors to see sufficient information regarding their own employees in government clearance databases so they can determine whom to propose for contracts.

IMPEDIMENTS TO RECIPROCITY WITH ALREADY CLEARED INDIVIDUALS

Government policies, practices, and resource allocations impede the movement of cleared federal contractors and government employees from one agency to another. Federal agencies are often reluctant to accept clearance decisions made by other agencies for three principal reasons:

1. Ambiguous or misinterpretation of policy and lack of oversight;
2. Inability to see the details behind other agency adjudicative decisions; and
3. Prioritization of government resources allocated to security processing.

> Individual contractors who move from one firm to another often wait weeks or months for their clearances to transfer to their new employer, during which time they cannot do work to support a classified contract.

While these impediments undermine the effectiveness of both federal workers and contractors, the impacts are amplified in industry, where these inefficiencies hinder the delivery of the services requested by the government. The resulting loss of labor hours undermine the critical national security missions of the Defense Department and the Intelligence Community and drive up costs. Although reciprocity delays affect both cleared contractors and government employees, contractors must transfer their clearances much more frequently because they typically support projects at multiple agencies other than the one that granted, and thus "holds," their clearances. This paper thus focuses principally on the impact of reciprocity delays on contractors.

AMBIGUOUS POLICY AND LACK OF OVERSIGHT

The Director of National Intelligence (DNI), in the role of the Security Executive Agent (SecEA) for National Security and Sensitive Positions, has issued binding policy guidance regarding clearances and reciprocity. Despite the best of intentions, this guidance has not achieved uniform implementation at agencies across the Intelligence Community and the Department of Defense (DoD). In practice, individual agencies created internal policies and procedures based on their own interpretations of SecEA directives (SEADs). At larger agencies like the DoD, sub-departments including the Army, Navy, and Air Force have further promulgated their own interpretations of both ODNI and DoD policy. This practice of agency-specific policy interpretation creates a web of inconsistent rules that complicate reciprocal recognition of clearances.

Notwithstanding the potential misinterpretations of the formal ODNI guidance as it makes it way down its path to implementation, it is important to review some of the actual language from the national-level policy guidance to identify the resulting impediments.

Lack of Definition Leads to Ambiguity

The first potential ambiguity in policy comes from Intelligence Community Policy Guidance (ICPG) 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations* (October 2, 2008), which applies to intelligence agencies and other government entities designated to determine eligibility for access to sensitive compartmented information (SCI).[2] This document states that "IC Element[s] shall accept all in-scope security clearance or access determinations (without waivers, conditions, or deviations as defined herein)" (para. C.2). Although the ICPG defines many of the terms used throughout, it does not provide a definition for the words "shall accept," and multiple agencies have created preconditions that shape their acceptance of clearances granted by other organizations.

For some security offices, "accepting" a clearance means approving the employee to be briefed and start working immediately as soon as his/her eligibility can be confirmed in the system of record. Other security offices, however, may require the subject to fill out or update the standard security questionnaire (SF-86) and answer supplementary questions on an SCI Interview Form or a Foreign National Contact and Foreign Association Form – which differ from agency to agency – and even undergo a further screening interview. Only then will the local security representative, after reviewing this additional documentation, decide whether to accept the clearance eligibility that is already listed in the system of record or whether to require further reporting or investigation.

The words "shall accept" imply "without delay or further investigation or adjudication." However, unless the overseers of the ICPG actually inspect the practices of agencies' front line security offices, they would not know that their policy is, in fact, not being executed in such a manner. If the ICPG's intent is for agencies to grant reciprocal access without delay, the SecEA needs to publish clarifying policy guidance and take steps to oversee agencies' implementation.

The recently published Security Executive Agent Directive (SEAD) 7 seems to rephrase the ICPG 704.4 language with the same intent without further clarification. SEAD 7 states, "Reciprocity is the acknowledgement and acceptance of an existing background investigation conducted by an authorized investigative agency; the acceptance of a national security eligibility adjudication determined by an authorized adjudicative agency; and the acceptance of an active national security eligibility determination granted by an executive branch agency."[3] The SEAD does not define whether "acceptance" permits the imposition of additional requirements except for seven specified reasons why reciprocity can be delayed (para E.2).

[2] *Intelligence Community Policy Guidance (ICPG) 704.4, Reciprocity of Personnel Security Clearance and Access Determinations (October 2, 2008). As of February 20, 2018: https://www.dni.gov/files/documents/ICPG/icpg_704_4.pdf.*

[3] *Security Executive Agent Directive 7, Reciprocity of Background Investigations and National Security Adjudications (November 9, 2018), para E.1., p. 2. As of February 20, 2019: https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf.*

Added Requirements Cause Delays

ICPG 704.4 states that investigations less than seven years old are considered "in scope" as the basis for initial or continuing access. However, the ICPG also establishes another time guideline, specifying, "Upon accepting an investigation more than five years old, the receiving agency shall ensure that its investigative element has received all necessary documentation to conduct a periodic reinvestigation."

The intent appears to be for an agency to accept the individual's current in-scope clearance eligibility and allow the subject to be briefed and start working, after which – "upon accepting an investigation more than five years old" [now six years old] – the agency would collect the paperwork necessary to conduct the periodic reinvestigation. Such an interpretation would allow a person who had already been determined to be trustworthy and who could continue accessing classified information if they remained in place to begin working at a new agency while his/her dossier is updated. However, this ambiguous language has led agencies to take a range of approaches. Some agencies hold off on reciprocity until the PR paperwork is submitted, others wait until its receipt by the investigative agency is visible in the system of record, and others insist on waiting until the investigation is open and running.

While submitting new investigation paperwork prior to accepting an individual's current eligibility may seem like a reasonable request with minimal delay, in most cases it causes an extensive delay.

- It may take the subject days to collect all necessary records and fill out the request.
- For DoD clearances, it can take the subject's private sector employer several days to ensure the forms are accurate and complete prior to transmission to Defense Security Service (DSS).
- Depending on backlog and funding, DSS may not forward the case to the Investigative Service Provider (ISP) for up to several weeks.
- Once at the ISP, the case may not be opened for days or weeks.

Industry currently has many thousands of personnel who were cleared on one government contract but who must wait weeks or months before being allowed to work on a new contract. (One large firm alone reported that it currently had more than 700 employees waiting for clearance transfers, and that on average its employees wait 94 days for their clearances to be accepted by a new agency.) Similarly, individual contractors who move from one firm to another often wait weeks or months for their clearances to transfer to their new employer, during which time they cannot do work to support a classified contract. This amounts to thousands of lost mission hours of effort for the government and increased overhead cost for industry, which ultimately will get charged back to the government. If the intent was to grant access and then collect and ensure the periodic reinvestigation paperwork is submitted, the SecEA should publish clarifying guidance to guarantee that agencies interpret and implement the policy correctly and consistently. The SecEA should also take steps to oversee agencies' compliance with such revised guidance.

Procedures Lag Behind New Adjudicative Standards

ICPG 704.2, *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and other Controlled Access Program Information*, allowed personnel to keep their Top Secret (TS) Sensitive Compartment Information (SCI) clearance eligibility for 24 months after they have been debriefed from access.[4] The interpretation that a subject with current TS/SCI eligibility who now needs TS/SCI access must have had SCI access within the past 24-months is obsolete.

When the ICPG was published in 2008, the DNI had just become the Security Executive Agent for all security clearance levels; as a result, the language still specifically addressed the restoration of SCI access for personnel whose TS clearances remain in-scope. At a minimum, given that reporting requirements for those with SCI and TS clearance outlined in SEAD 3 are now identical, a break in service or access should allow for TS access to count in maintaining SCI eligibility. Further, now that the ICPG has been rescinded and the SEAD is silent on the matter, it appears that the government can no longer invalidate an otherwise valid eligibility after 24 months without access to classified information. Clarifying guidance should be published to ensure the policy is clear.

In Progress Periodic Reinvestigations and Unadjudicated Clean PRs Delay Reciprocity

ICPG 704.4 states that "eligibility for access determinations shall be mutually acceptable throughout IC security elements and shall not be re-adjudicated unless… New information has surfaced since the last investigation that indicates the subject may not satisfy the adjudicative requirements…"[5] However, some IC elements consider an in-progress PR or a completed but unadjudicated PR to be sufficient to deny reciprocity of current clearance eligibility.

The policy seems to clearly suggest that only newly discovered derogatory information should delay reciprocity, not a running PR or a completed one not flagged as derogatory. At the National Security Agency (NSA), completed periodic reinvestigations may remain unadjudicated for two to three years if there is no sign of derogatory information due to the prioritization of initial clearance investigations. This leaves many personnel ineligible for reciprocity for several years. Even though SEAD 7 appears to require having knowledge of derogatory information before stopping reciprocity, this is often not the practice.

Duplicating Adjudication and Transfers of Clearance Data Wastes Resources

There is a lack of policy from DoD on the adjudication of Single Scope Background Investigations (SSBIs) and Tier 5 (T5) investigations – required for access to Top Secret/SCI – by DoD's consolidated adjudication facility (DoDCAF). Specifically, as a matter of practice, when a contractor's SSBI/T5 investigation is completed and forwarded to the DoDCAF for adjudication, if the subject is not at that point in time "owned" by an Intelligence Special Security Office (SSO) in the Joint Personnel Adjudication System (JPAS), the DoD clearance information system of record, the DoDCAF will only adjudicate the case to the TS level, even if the request was for TS/SCI access.

[4] *ICPG 704.2, Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and other Controlled Access Program Information (October 4, 2008), para C.3. As of February 20, 2019: https://www.dni.gov/files/documents/ICPG/ICPG_704_2.pdf.*

[5] *ICPG 704.4, para C.7.*

Once the DoDCAF grants TS eligibility, industry must then forward a separate SCI nomination request to the government SSO, who in turn will have to request a second adjudication from the DoDCAF for TS/SCI. With the 2017 publication of SEAD 4 *(National Security Adjudication Guidelines)*, the adjudicative standards for TS and TS/SCI are identical. With average adjudication timelines at the DoDCAF now approximating 30 days, this practice delays thousands of contractors from supporting DoD missions by a month or more per person. Furthermore, by requiring two adjudications to identical standards for the same individual, this DoDCAF practice literally doubles the workload of DoDCAF personnel for these case types.

Additionally, the DoDCAF has a practice of responding to contractor requests to move TS/SCI eligibility from Scattered Castles (SC) – the Intelligence Community's security database – to JPAS in the same redundant manner. DoDCAF will only transfer the TS portion and then wait for industry to once again submit a request through the government SSO to generate a second request to transfer the SCI portion. Here we have another delay of one to two months for individuals who are for the most part, already working on TS/SCI cleared contracts.

Replacing Periodic Reinvestigations with Continuous Evaluation Introduced New Roadblocks

In 2018, DoD decided to defer T3[6] and T5 periodic reinvestigations that do not contain derogatory information and instead use Continuous Evaluation (CE), a set of primarily automated record checks, to monitor the behavior of cleared individuals on an ongoing basis. This decision replaced burdensome and time-consuming reinvestigation requirements with an automated process that would, theoretically, identify potentially derogatory information in real time. Furthermore, replacing PRs with CE enrollment allowed background investigators to focus on a backlog of more than 700,000 investigations that hindered hiring across government and industry.[7] However, it has also led to a series of impediments to timely reciprocity.

> Without the SecEA enforcing reciprocity, and without the DoD making CE enrollments visible to all government security offices, what was intended as a means to reduce the investigation backlog is creating a reciprocity crisis.

DoD did not make evidence available to anyone except the investigation requestor that it had enrolled the subject in CE. While DoD did commit to modifying the Department's system of record to add this new information by the end of 2018, DoD officials asserted it could be more than a year before that information would be visible to non-DoD security personnel. This means non-DoD agencies would only have the word of a private company that its employee is enrolled in CE; not surprisingly, these agencies often decline to accept such assurances and thus refuse to grant reciprocity to personnel whose investigation is out of scope, even though enrollment in CE removed the requirement for a PR.

[6] *Tier 3 (T3) investigations are required for access to Confidential or Secret information.*

[7] *Patrick Tucker, "US Plans 'Continuous Evaluation' of New and Existing Security Clearances," DefenseOne, July 12, 2018. As of February 20, 2019: https://www.defenseone.com/technology/2018/07/us-plans-continuous-evaluation-new-and-existing-security-clearances/149693/.*

This lack of transparency on CE enrollment also hinders individual contractors who seek to change employers. Because an individual enrolled in CE would not go through a PR at the mandated time, a potential new employer would assume the person's clearance was out-of-scope, as it would have no evidence that its new employee had been enrolled in CE. A firm might decide not to hire someone whose investigation appears, erroneously, to be out-of-scope, leaving contractors enrolled in DoD continuous evaluation to be, in practice, trapped at their current employers. Such a dynamic prevents cleared labor from being allocated where it is most effective.

Even more concerning is the expressed refusal of senior security officials to accept DoD CE enrollment. During a panel discussion on October 24, 2018 at the National Defense Industrial Association conference, several IC Security Directors indicated they would not accept and cross over a subject with TS/SCI eligibility whose investigation was more than 7 years old but was enrolled in DoD CE.

Without the SecEA enforcing reciprocity, and without the DoD making CE enrollments visible to all government security offices, what was intended as a means to reduce the investigation backlog is creating a reciprocity crisis.

INABILITY TO SEE DETAILS BEHIND OTHER AGENCY DECISIONS

At the core of many reciprocity delays is the inability of federal agencies to see the rationale for the clearance eligibility decisions made by other agencies. There are two principal aspects and consequences to this challenge. First, given that agency contracts often require industry to propose personnel who meet very specific clearance criteria, a firm may not know if its employees are eligible because of its limited access to government systems of records and its inability to predict if an agency will accept an adjudication decision by another agency.

Second, government agencies often cannot see the details behind the investigative and adjudicative records of other agencies, which often makes them reluctant to grant reciprocal access.

- ICD 704 states that "the IC Scattered Castles repository, or successor database, shall be the authoritative source for personnel security access approval verifications regarding SCI and other controlled access programs, visit certifications, and documented exceptions to personnel security standards. Heads of IC Elements shall ensure that accurate, comprehensive, relevant, and timely data are delivered to this repository. Specific guidelines are contained in ICPG 704.5."[8]
- ICPG 704.5 further provides that the ODNI's Special Security Center shall "collaborate with the Department of Defense and the Office of Personnel Management (OPM) to ensure Senior Officials of the Intelligence Community-approved personnel security information contained in the SC database is accessible and the data is correlated with OPM's Clearance Verification System database at the appropriate level of classification to protect agency-specific classified information."[9]

These policies seem clear in their intent that clearance eligibility decisions and exceptions should be clearly documented. The SEAD requires ODNI, DoD and OPM to ensure "information in the SC database is accessible." However, it appears that in the case of SC, some government agencies are reluctant to make the information "accessible" to industry, which has two major implications.

[8] *Intelligence Community Directive (ICD) 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (October 1, 2008), para. D.7.d. As of February 20, 2019: https://www.dni.gov/files/documents/ICD/ICD_704.pdf.*

[9] *Intelligence Community Policy Guidance (ICPG) 704.5, Intelligence Community Personnel Security Database Scattered Castles (October 2, 2008), para. E.1.a. As of February 20, 2019: https://www.dni.gov/files/documents/ICPG/icpg_704_5.pdf.*

1. Insufficient Industry Access to Scattered Castles Data Hampers Submission of Eligible Transfers

The first is that lack of SC access impedes contractors' ability to propose candidates who will move quickly through the system, meet government requirements, and satisfy industry business needs to keep cleared assets actively working on contracts. All classified U.S. Government contracts have clearance and or polygraph requirements that must be met to perform on the contract. One such requirement may state that all personnel must have a SSBI completed within the last five years with TS/SCI eligibility and a favorably completed Counterintelligence Scope Polygraph examination. However, the ODNI has authorized individual agencies to limit or even prohibit contractor access to the SC that contains the information needed to comply with government contract requirements. Without such data, a firm may inadvertently propose a candidate that does not meet government requirements, leading to wasted weeks or months while the contractor waits, then recruits a new candidate believed to meet the requirements, and starts the process again.

For cleared companies to meet contractual requirements, they need to have access to SC at a scale sufficient to verify the nearly 180,000 individuals who are hired or moved from one contract to another every year. They should be able to see five data points within the system(s):

1. The date and type of investigation with the conducting agency;
2. The date and level of clearance eligibility and the granting agency;
3. Whether the eligibility was based on an exception (but not details about the exception);
4. The date of last access to comply with break-in-access rules if the break in service continues to be an issue; and
5. The date and type of successfully completed polygraphs.

> For companies to meet contractual and policy requirements, agency processes should make SC data accessible and enable cleared industry companies to submit qualified personnel.

In most cases, cleared industry companies do not have access to this level of information, even though their contracts with the government require them to propose and submit only personnel whose compliance with certain criteria can only be confirmed by comprehensive SC access. This "Catch-22" has a number of bad results:

- A company can lose a contract because it failed to provide sufficient numbers of adequately cleared personnel.
- Post-award records checks performed by the government acquisition authority can identify personnel who do not meet the requirements causing the contractor to terminate and rescind hiring offers and start the recruiting process again, delaying full staffing of the government's needs.

For companies to meet contractual and policy requirements, agency processes should make five SC data accessible and enable cleared industry companies to submit qualified personnel. For this to happen, ODNI should require IC agencies to authorize equal access to the SC data elements identified in this report to companies appropriately cleared security representatives.

2. Government Data Sharing Is Inefficient

The second challenge is government agencies' inability to see the details behind other agencies' investigative and adjudicative records. To overcome this shortfall and onboard cleared contractors in a timely manner, the agencies need access to Scattered Castles; DoD's Joint Personnel Adjudication System (JPAS) and its successor, Defense Information System for Security (DISS); OPM's Central Verification System (CVS); and the verification systems of other federal agencies in order to successfully onboard cleared contractors in a timely manner.

When cleared contractors move from one agency to another, the responsibility for the risk transfers, but the level of risk usually stays the same because the adjudication standards do not change. However, SEAD 7 is being interpreted by implementors in a way that entrenches agencies' ability to vary and thereby lengthen the decisionmaking process. The document states, "agencies may request the covered individual to identify any changes since the last SF-86 submission… Agencies may conduct the appropriate personnel security interview or inquiry pertaining to the changes" (para. E.1.d). This language opens the door to any security officer making his/her own determination and not immediately accepting the system of record eligibility because agencies have no visibility to previously reported and adjudicated information.

Timeframes for clearance transfers can already take months, and the challenge becomes even greater for cases that are decided based on exception, and therefore do not meet the standard for mandatory reciprocity. For the thousands of cases that are decided based on exception (waivers, deviations and conditions), the adjudicative challenge becomes even greater, as decisions to grant eligibility are valid only at the agency where the adjudicative decision was made. To assign such an employee to a contract supporting another agency requires a company to request a crossover of the clearance, which can take months to complete.

The only information another security officer is able to see in SC is the fact that the adjudication was made by exception; he or she cannot see details regarding the cause or the rationale for mitigation. Therefore, the gaining agency must request a copy of the last investigation to conduct their own adjudication.

Three case studies show how different agencies apply their own rules to crossover requests.

- In the case of a DoDCAF adjudication being considered by another agency, the investigation was likely done by the National Background Investigation Bureau (NBIB). A request must go to NBIB for the investigative file, which can take several weeks for a hard copy file to be received. The new SEAD 7 requirement for ISPs to respond within 10 business days is better than not having any time requirement but is still not an optimal standard. Those files then go into the agency's adjudicative queue, where they may linger for many more weeks. It is not uncommon for these cases to take one to three months to resolve. SEAD 7 also requires reciprocity decisions to be rendered in five business days, yet it is unclear at what point in the process these five days are measured. Moreover, cases adjudicated by exception do not meet mandatory reciprocity standards and therefore are not subject to the five-day standard.

- In the case of National Geospatial-Intelligence Agency (NGA), when the agency determines it must order the case, it rejects industry's request for crossover. NGA then asks the industry employer to refrain from submitting a new request until the agency notifies the employer that it has received the investigation file.

- In the case of the Central Intelligence Agency (CIA) and the DNI's Community Program, when the agency realizes it must order the case, it rejects industry's request for a crossover and recommends industry resubmit the request as an initial clearance; this request goes into the queue with all other initial clearances, which can take upwards of one year to ultimately get adjudicated.

These practices of creating internal agency procedures obscure the true length of time to respond to reciprocity requests. If policy required full documentation in the adjudicative record – and the ODNI policies do seem to imply as much – none of these agencies would need to go back to the original investigation.

As an alternative, DoD IC agencies could log into the DoDCAF Case Adjudication Tracking System (CATS) and review the decision that was made by the DoD adjudicator. In theory, this system lists all contentious issues from the investigation and provides the mitigation rationale used by the adjudicator. It appears this change would simply require creating user accounts for the adjudicators at the DoD IC agencies, who by definition are DoD adjudicators. If implemented, it could significantly reduce the adjudicative backlog and eliminate weeks to months of delays in granting reciprocal access, thereby enabling thousands of contract personnel to begin work on government priorities. If this solution is accepted, the government could expedite access to the DoD's systems of record (CATS and DISS) to other federal adjudicators, thereby eliminating these delays government-wide.

While not directly related to security clearances, greater information-sharing among agencies could significantly reduce the time needed to conduct Public Trust or suitability determinations. Because agencies cannot see adjudicative records to see details of behavior that might be disqualifying for certain jobs – the Drug Enforcement Administration (DEA) might consider drug use disqualifying, for example, even if other agencies do not – agencies tend to run duplicative background investigations on personnel who already hold clearances.

RESOURCE PRIORITIZATION

A lack of government resources and the inefficient prioritization of those limited resources negatively impact the timeliness of clearance reciprocity. As an example, while the NSA is working to get new hires, who have no clearance and no polygraph, ready to work in six months, those who already have a clearance fare far worse. In fact, it generally takes TS/SCI-cleared contractors working on a DoD contract several months – and as many as 12 to 18 months – just to schedule the polygraph required to work on an NSA contract. According to NSA, it has prioritized its limited polygraph resources to focus first on newly hired federal employees who require an initial clearance decision and then, secondarily, on contractors who require an initial clearance decision. The reason is a combination of internal priorities and the need to be responsive to performance metrics. Similar processes and waiting periods exist at CIA and ODNI.

NSA, like other federal agencies, has performance goals derived from the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). However, cleared personnel who simply need a polygraph do not appear to fall under IRTPA performance goals. Moreover, SEAD 7 provides policy top cover for polygraph delays, stating, "The additional processing time for completion and adjudication of the polygraph examination shall not be counted as processing time for the reciprocity determination" (para. E.4). This resource prioritization and policy generate two outcomes: First, contractors are delayed getting to work for the government. Second, companies often propose personnel based on their clearances rather than on their skills and qualifications. (Both government and industry prefer an adequate employee with a polygraph who can start work immediately over a highly qualified candidate who cannot start work for many months.) Neither of these outcomes is best for government or industry.

If agencies continue to have polygraph requirements, they should be funded and staffed sufficiently to process such requirements in a timely manner. (Of course, when polygraph delays are not counted toward timeliness requirements, such delays are not reflected in agency performance metrics that are used to identify the need for additional resources.) Ultimately, waits of more than a year for a TS/SCI-cleared contractor to get a polygraph scheduled, completed and adjudicated undermine the effectiveness of government agencies.

Mission Impact and Cost

The government does not routinely or methodically collect performance data that could identify systemic delays in processing reciprocity requests or obsolete and redundant procedures. The lack of metrics makes it difficult to improve the effectiveness of its operations. One potential reason is that most policy makers and overseers – SecEA/ODNI, DoD, and the PAC Program Management Office (PMO) – are understandably predisposed to measure the effectiveness of policies based on intended rather than actual outcomes. It would likely not occur to policy makers to ask, for example, if the same person was adjudicated twice to the same standard or if requests for reciprocity are reclassified as initial adjudications. One of the intended outcomes of this paper is to provide sufficient information to help policy makers and overseers begin to collect meaningful metrics and better understand actual outcomes.

It is difficult to quantify the impact of reciprocity delays, as salaries vary widely by firm, contract, level of experience, and clearance. Nevertheless, we can make some rough estimates. In the Intelligence Community, industry leaders estimate that roughly 10 percent of the cleared contractor labor force is idle at any given time because they are waiting for a clearance to be granted, updated, or transferred. Given that the average cost to the government of an individual TS/SCI-cleared contractor (many of whom have passed polygraphs as well) is approximately $200,000 per year (a figure that includes salary, benefits, and other overhead cost), the cost of this idle labor to the Intelligence Community alone approaches $2 billion per year and 1,000 labor-years.[10]

[10] A compensation survey undertaken in 2018 by ClearanceJobs.com, a news and employment site for cleared government employees and contractors, reported that the average total compensation for professionals with TS/SCI clearances was $99,035, and the average compensation for professionals holding "intelligence clearances" (TS/SCI with a polygraph) was $122,243. Add the cost of benefits (roughly 46 percent of wages and salaries for management and professional workers, according to the Bureau of Labor Statistics), plus overhead and related expenses, and $200,000 is a reasonable estimate for the average burdened cost of a cleared contractor. See The Big Thaw: A Comprehensive Earnings Survey of Security-Cleared Professionals, ClearanceJobs.com, 2018, p. 8. As of February 20, 2019: https://clearance-jobs-assets.s3.amazonaws.com/customer/2018CompensationReport_ONLINE.pdf. See also Bureau of Labor Statistics, "Employer Costs for Employee Compensation – September 2018," news release, USDL-18-1941, December 14, 2018. As of March 5, 2019: https://www.bls.gov/news.release/ecec.nr0.htm. For statistics related to management and professional workers, see "Table 1. Civilian workers, by major occupational and industry group." As of March 5, 2019: https://www.bls.gov/news.release/ecec.t01.htm.

> ...industry leaders estimate that roughly 10 percent of the cleared contractor labor force is idle at any given time because they are waiting for a clearance to be granted, updated, or transferred... the cost of this idle labor to the Intelligence Community alone approaches $2 billion per year and 1,000 labor-years.

Extrapolating to the entire U.S. Government, which engages more than 900,000 cleared individual contractors, the cost would be far higher.[11] If a similar percentage of the contractor labor force is idle while clearances are being processed, that means roughly 90,000 labor-years are lost to processing time. A compensation survey undertaken in 2018 by *ClearanceJobs.com*, a news and employment site for cleared government employees and contractors, reported that the average total compensation for worldwide cleared professionals (both government employees and contractors holding any level of security clearance) was $93,004.[12] Using this average compensation figure – which does not even factor in benefits and overhead expense for contractors – the cost to the entire federal government of 90,000 labor years lost solely to clearance delays would total $8.37 billion per year.

One can certainly debate the assumptions and the math used to calculate these costs, but it is unquestionable that the described inefficiencies undermine the national security mission and yield significant unnecessary costs. The end result is that the national security mission suffers because of delays in the investigation and adjudication processes, as well as the systemic delays surrounding reciprocity. The government is getting access to those who can afford to wait for the delays to sort themselves out, but they are not enough to fill the requirements. Moreover, these delays and obstacles lead to a sub-optimal allocation of labor; individuals may be assigned to a project not because their skills make them ideally suited for it, but because their clearances enable them to start working right away.

[11] *According to the ODNI, approximately 925,000 contractors held security clearances at the end of FY2015 (September 30, 2016). See Office of the Director of National Intelligence, 2015 Annual Report on Security Clearance Determinations, no date, p. 5. At https://www.odni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2015-Annual_Report_on_Security_Clearance_Determinations.pdf.*

[12] *The Big Thaw: A Comprehensive Earnings Survey of Security-Cleared Professionals, ClearanceJobs.com, 2018, p. 3. As of February 20, 2019: https://clearance-jobs-assets.s3.amazonaws.com/customer/2018CompensationReport_ONLINE.pdf.*

RECOMMENDATIONS

A determination by the SecEA and individual agencies to fix the following 14 policy and process inefficiencies will generate improved results, cost savings, and national security impact for the Intelligence Community, the Defense Department, and U.S. taxpayers.

1. Clarify the implementor's perception of "shall accept" in reference to reciprocity of non-exception cases to mean that

    A. Personnel with valid eligibility and in-scope investigations (currently seven years) will be brought on board and briefed without delay or additional paperwork, and that

    B. Any additional paperwork authorized by the ICPGs or the SEAD be collected after on-boarding or after the subject has started cleared work at his/her new agency or contract.

2. Require the DoDCAF to adjudicate all SSBI/T5 cases to the TS/SCI level (rather than to the TS level) based on one request from industry, without requiring a second request from the government.

3. Require the DoDCAF to cross-over all non-exception TS/SCI cases from SC to JPAS based on the first request from industry (without requiring a second request from the government), even if the government has yet to establish an SCI-owning relationship.

4. Prohibit in-progress or un-adjudicated PRs that are not flagged as derogatory from being used to stop reciprocity and negate current eligibility.

5. Issue NSA, NGA, DIA, NRO and CIA adjudicators read-only accounts in the DoD adjudicator database so they can see the rationale and mitigation for exception cases, which would eliminate the requirement for these agencies to order the original investigation from NBIB.

6. Issue DoDCAF SCI-cleared adjudicators read-only accounts on intelligence agency adjudication systems so they can see the rationale and mitigation for exceptions cases, which would eliminate the requirement to order the original investigation from multiple sources.

7. Direct intelligence agencies to provide industry sufficient numbers and levels of SC accounts to allow firms to make clearance and reciprocity determinations for new hires based on government contract requirements.

8. For those agencies that require polygraphs, ensure they are funded and staffed to complete ALL polygraphs within 30 days. In the interim, require those agencies to on-board and provide full access to TS/SCI-cleared personnel within 30 days, even if the polygraph is not completed.

9. Sufficiently staff and fund NSA to eliminate the years-long backlog of pending PR adjudications.

10. Allow those with non-exception TS/SCI eligibility but only TS access in the last 24 months to be briefed into SCI without delay and/or announce the elimination of the 24-month break in service restriction.

11. Make the enrollment of personnel in CE in lieu of a PR visible to both government agencies and industry in JPAS, DISS, SC and CVS.

12. Require all government agencies, including intelligence agencies, to grant reciprocity without delay or additional paperwork for individuals who are TS/SCI-eligible when the subject is enrolled in CE but has an investigation that is older than seven years.

13. Resource government adjudication facilities to the level needed to meet the timeliness requirements of SEAD 7 and augment the DoDCAF with contractors to migrate non-exception adjudications into JPAS, since moving data is not inherently governmental.

14. Augment the ODNI security staff to enable an appropriate level of oversight for what is now a federal government-wide mission rather than one limited to the IC.

While the above recommendations will resolve many of the obstacles to true reciprocity, it is appropriate that agencies and cleared industry firms report true violations of DNI reciprocity rules to SECEA@DNI.GOV. This address should not be used to resolve employee-specific clearance issues.

FINAL THOUGHTS

Implementation of these recommendations will:

- Identify practical impediments to efficient reciprocal recognition of clearances and direct agencies to remove such impediments;
- Use available technology to increase the speed at which reciprocity decisions can be made;
- Resource all government adjudication and polygraph staffs to levels needed to meet appropriate timeliness goals, including on-boarding of currently cleared personnel within 30 days;
- Enable currently cleared contractors and government employees to begin work at a new agency while additional information is collected and adjudicated;
- Prevent the adjudication of individuals to the same standard twice;
- Require greater information-sharing regarding personnel clearances among agencies and between government agencies and their industry partners, as a lack of transparency prevents security officers from trusting other agencies' clearance decisions; and
- Enable contractors to see sufficient information regarding their own employees in government clearance databases so they can determine whom to propose for contracts.

The president signed an Executive Order that establishes a new agency, the Defense Counterintelligence and Security Agency (DCSA), that will consolidate many security clearance related responsibilities within one organization with government-wide responsibilities. While this reform may alleviate some challenges, it will not, by itself, fix the fundamental reciprocity issues identified in this paper. Only a comprehensive effort by the Security Executive Agent to fix these ambiguous and conflicting policies and practices can do that.

This paper identifies the most important challenges and suggests steps to mitigate these challenges and improve reciprocity across the IC and across government. The results of fundamental reform to this process will be improved efficiency, significant cost savings, and better retention of critical talent in both government and industry.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.

ABOUT INSA'S SECURITY POLICY REFORM COUNCIL

INSA's Security Policy Reform Council seeks to transform the paradigms that govern the design and execution of security policy and programs and to serve as a thought leader on security issues. The Council works with industry and government stakeholders to identify and mitigate security challenges, develop security solutions, and advocate for security reforms to enhance industry's ability to support and protect national security.

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org