



SAME BUT DIFFERENT: *Security Clearances for Contractors and Government Employees*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Insider Threat Subcommittee

January 2020



INSIDER THREAT
SUBCOMMITTEE



ABBREVIATIONS

BI	Background Investigation	FIS	Federal Investigative Standards
CAF	Consolidated Adjudication Facility	IC	Intelligence Community
CE	Continuous Evaluation	JVS	Joint Verification System
COTR	Contracting Officer Technical Representative	JPAS	Joint Personnel Adjudication System
CV	Continuous Vetting	NISPOM	National Industrial Security Program Operating Manual
DCSA	Defense Counterintelligence and Security Agency	NSA	National Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement	PAEI	Publicly Available Electronic Information
DoD	Department of Defense	PR	Periodic Reinvestigation
DODCAF	Department of Defense Consolidated Adjudications Facility	SAP	Special Access Program
DOJ	Department of Justice	SC	Scattered Castles
FAR	Federal Acquisition Regulations	SCI	Sensitive Compartmented Information
		TS	Top Secret

EXECUTIVE SUMMARY

Both government employees and contractors who require a security clearance are subject to comprehensive vetting and periodic reinvestigation or Continuous Evaluation (CE) of their behavior. Government policy requires both go through the same vetting and adjudication process. However, INSA has found two critical differences when it comes to how contractors and government employees are monitored on an ongoing basis (through continuous vetting (CV)* or insider threat monitoring):

1. **SOCIAL MEDIA:** Individual government contractors face more rigorous scrutiny, as private companies can monitor employee's social media as part of their continuous vetting and insider threat protocols. However, despite the existence of a directive permitting them to do so, government agencies do not monitor their employees' social media. Our interviews found this is due to a lack of clear guidance on how to implement the existing directives and security policies. This shortcoming can be remedied by government agencies agreeing upon a single common standard regarding the use of publicly available electronic information, specifically social media, for personnel security and insider threat purposes. The DNI, as Security Executive Agent for the government, must then develop guidelines for the implementation of this standard throughout the sector.
2. **INFORMATION-SHARING:** Currently, only contractors share information regarding at-risk employees. The government does not share with industry when they identify a "red flag" about a contract employee working at a federal facility. This unwillingness to share data prevents the employee's firm from mitigating the potential risk. Government's reluctance is rooted in a lack of clarity regarding the types of information that can be shared under the Privacy Act of 1974. In contrast, reports of adverse behavior by government employees are entered into appropriate security databases and follow them from employer to employer, as long as they continue working for the government. Intelligence agencies, in coordination with the Department of Justice (DOJ), must agree on a uniform government-wide interpretation of what information sharing is permitted under the Privacy Act. Should changes to this statute be required to address security risks, the Administration should propose such changes to Congress.

In addition, current Federal Acquisition Regulations (FAR), constrain communications between government managers and their contractors. Changing the FAR, could permit more comprehensive and rapid sharing of information on personnel security risks.

* Continuous Evaluation (CE) involves a check of seven specific data categories. Continuous Vetting is CE plus reviews of internal data sources.

KEY FINDINGS

Interviews with both government and industry officials yielded several insights of interest to illustrate ways the vetting of contractors and government employees are similar and different:

- Contractors and government employees undergo identical background investigation (BI) and adjudication processes to obtain a security clearance.
- Suitability and fitness determination processes are essentially the same for government and contractor personnel. Both contractors and government employees are measured against the same overall standards.
- Contractors are subjected to greater scrutiny in one respect – private companies can conduct social media monitoring of their employees as part of their continuous vetting and insider threat protocols. However, despite the existence of a directive permitting them to do so, Government agencies do not monitor their employees' social media because there is no clear guidance on how to implement the existing directives and security policies.
- No single common standard exists regarding the use of publicly available electronic information, specifically social media, for personnel security and insider threat purposes. The DNI, as Security Executive Agent for the government, must then develop guidelines for the implementation of this standard throughout the sector.
- Currently, only contractors share information regarding at-risk employees. Due to a lack of clarity regarding the types of information that government can legally share with contractors, agencies fail to inform contracting firms that their employees have raised security concerns. This lack of information-sharing prevents firms from effectively monitoring risks posed by their employees and taking corrective action. It also enables individuals who have been identified as potentially posing security risks to change firms without either company knowing of the allegations.
 - In contrast, reports of adverse behavior by government employees that are entered into appropriate security databases follow them from employer to employer as long as they continue working for the government.
- A higher share of contractors are subject to comprehensive continuous monitoring than federal employees. This is because all cleared contractors must have insider threat programs while only some government agencies have enrolled personnel in Continuous Evaluation (CE) programs.

BACKGROUND

Personnel performing classified work generally receive a security clearance at the Secret or the Top Secret (TS) level. Beyond that, access can be granted to Sensitive Compartmented Information (SCI) and to Special Access Programs (SAPs), to which access is even more limited. Although multiple agencies can conduct personnel background investigations and adjudicate clearances, this paper is focused on those clearances issued by the Department of Defense (DoD) and the Intelligence Community (IC), which represent the vast majority of the approximately four million clearances issued.¹

Figure 1 shows the high-level lifecycle of a security clearance for both government employees and contractors. The clearance process consists of five stages: initiation, a "suitability" or "fitness" determination, a background investigation, adjudication, and occasional reassessments in the form of a Periodic Reinvestigation (PR) or Continuous Evaluation (CE). The process is undertaken by the government regardless of whether the person seeking a clearance is a government employee or a private contractor.

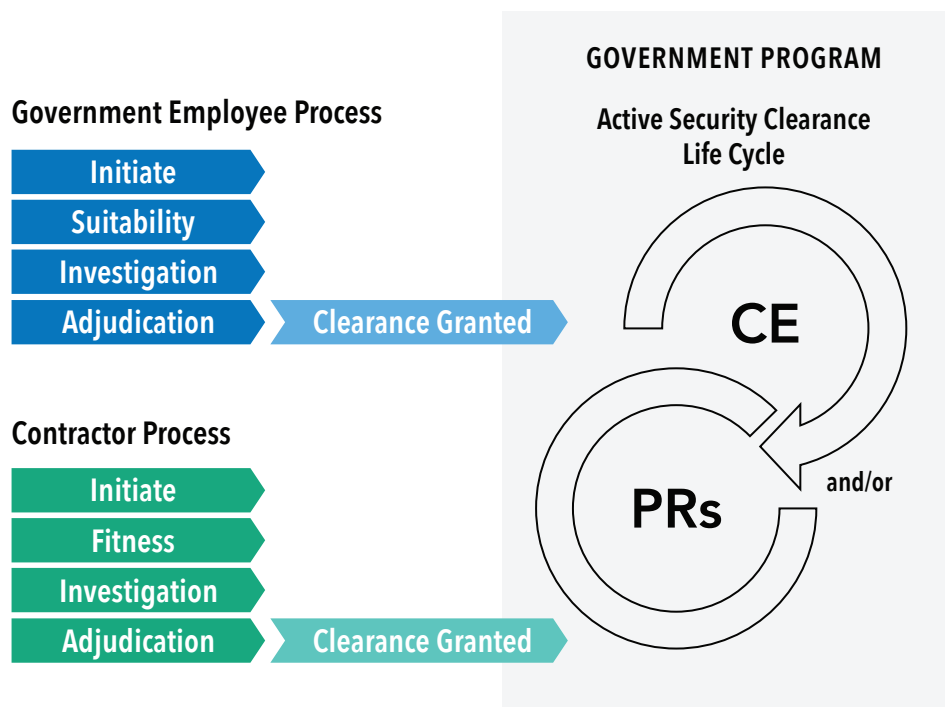


Figure 1 - Government Employee vs. Contractor Clearance Process

¹ National Counterintelligence and Security Center, Office of the Director of National Intelligence, Fiscal Year 2017 Annual Report on Security Clearance Determinations, August 2018, p. 5. Data as of October 1, 2017. At <https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf>.



Government employees and contractors go through the same background investigation processes, and the same rigor is applied to both populations.

- 1. INITIATION:** A clearance investigation is initiated when (a) a candidate receives an offer of a government job that requires access to classified information, or (b) when a private sector employee is placed on a contract requiring classified access and the supported government agency agrees to sponsor the individual for a clearance.
- 2. SUITABILITY/FITNESS:** Both government employees and contractors seeking a clearance must be deemed to have integrity and good character. Suitability determinations (for government employees) and fitness determinations (for contractors) are essentially the same despite the differences in terminology² – they assess whether an individual is suitable (or fit) for employment by (or contract to) the federal government. Most agencies conduct suitability and fitness determinations as part of background investigations, but the determination itself is a discrete stage in the process.
- 3. INVESTIGATION:** Government employees and contractors go through the same background investigation processes, and the same rigor is applied to both populations. The process includes review of a comprehensive form (the SF-86) submitted by the candidate, database checks, and interviews with the candidate and with his/her co-workers, neighbors, and other personal and professional contacts.
- 4. ADJUDICATION:** While standard adjudicative criteria exist, multiple adjudicating organizations exist, and their processes may vary.³ While processes may differ by agency, each agency subjects both government employees and contract employees to the same adjudicative process and evaluates them against the same adjudicative standards before granting them clearances.
- 5. POST-CLEARANCE REINVESTIGATION OR CONTINUOUS EVALUATION:** All cleared personnel are required to undergo a Periodic Reinvestigation (PR); TS-cleared personnel undergo a PR every five years, while Secret-cleared personnel get a PR every ten years. Some agencies are beginning to enroll personnel in Continuous Evaluation (CE) in lieu of PRs. CE, which uses automated database checks to identify concerning behavior in near-real time, mitigates the risk that an employee or contractor could engage in unnoticed misconduct in between investigations.

¹ National Counterintelligence and Security Center, Office of the Director of National Intelligence, *Fiscal Year 2017 Annual Report on Security Clearance Determinations*, August 2018, p. 5. Data as of October 1, 2017. At <https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf>.

² One difference: Candidates for government jobs may have to undergo drug testing and/or a psychological examination for Suitability Determinations, whereas contractors do not have to do so for Fitness Determinations. That said, both drug use and psychological issues are examined by investigators and evaluated by adjudicators later in the clearance process for both populations, so this difference does not mean that government employees undergo greater overall scrutiny than their contractor counterparts.

³ The DoD Consolidated Adjudications Facility (DODCAF), for example, is the sole authority in DoD to determine the security clearance eligibility of non-intelligence element DoD personnel occupying sensitive positions or requiring access to classified material. Intelligence agencies have their own adjudicating organizations and are focused on TS-cleared personnel with SCI access, many of whom also require Counterintelligence or Full Scope (“lifestyle”) polygraph examinations.

FINDINGS

VETTING PROCESSES ARE VIRTUALLY IDENTICAL

Interviews with both government and industry officials found that contractors and government employees undergo the same background investigation and adjudication processes to obtain a security clearance. All applicants fill out the same SF-86 form, all have background investigations following the same Federal Investigative Standards (FIS), and all are adjudicated following the same 13 national security adjudicative guidelines. There are, however, some differences, especially with respect to Fitness and Suitability.

Some government officials interviewed believed that suitability is more comprehensive for government employees than fitness is for contractors. However, in practice the differences are minimal.

- Government employees are required to take a drug test as part of Suitability determinations, whereas contractors are not required to do so as part of a fitness determination. However, whether a government applicant tests positive in the suitability review or a contractor applicant is found to use drugs during pre-employment screening – or whether either person is found to use drugs during a background investigation – neither person would be hired.
- Several IC agencies require a psychological evaluation to assess suitability of government employees. Contractors are not required to undergo psychological testing for fitness determinations, and few, if any, companies routinely administer psychological screening of their own employees. However, anyone (government or contractor) who acknowledges seeking counseling during the background investigation stage will be evaluated to see if their psychological issues pose a potential security threat. Furthermore, certain intelligence agencies require psychological screening of all personnel seeking high-level security clearances.

Continuous Monitoring is More Rigorous in Industry

Not all agencies have CE programs. Those that do employ different processes, though all meet the minimum standards set by the Director of National Intelligence (DNI) in Security Executive Agent Directive-6 (SEAD-6). Currently, only 1.4 million federal employees are currently enrolled in CE programs in the IC and DoD.⁴

In contrast, as of 2016, all cleared contractors have been required to implement comprehensive insider threat programs that monitor employees' behavior and identify potential risks. While each company has its own process, all cleared contractors' programs must meet minimum standards set by the National Industrial Security Program Operating Manual (NISPOM).⁵ While not generally referred to as "continuous evaluation," these industrial insider threat programs do continually evaluate the firms' employees.

Continuous vetting of contractors is more stringent, particularly at large companies that employ sophisticated programs, in one crucial way: Contractors can collect social media data regarding their employees, whereas government agencies have taken the position that privacy-related statutes prevent them from collecting similar information regarding government employees.⁶ This is a critical difference, because social media postings and publicly available electronic information (PAEI) contain information that is highly relevant to adjudicative guidelines, especially those regarding past personal conduct.⁷ Social media postings in particular can also provide insights into potentially concerning future behavior, which can serve as the basis for providing counseling or other assistance to an employee before a problem arises.

⁴ Tricia Stokes, Director, Defense Vetting, Defense Counterintelligence and Security Agency, remarks at Intelligence and National Security Summit, National Harbor, MD, September 5, 2019.

⁵ Conforming Change 2 to the National Industrial Security Operating Manual (NISPOM) required cleared contractors to establish comprehensive insider threat programs and set standards for these programs. See Defense Security Service, Industrial Security Letter ISL-2016-02, May 21, 2016. At <https://cdn2.hubspot.net/hubfs/283820/ISL2016-02.pdf>.

⁶ Government policy actually does permit agencies to collect social media data, but agencies have refrained from doing so because of a lack of guidance regarding how to navigate privacy concerns. While Security Executive Agent Directive 5 (SEAD-5) provided the authority to collect social media for BIs, it did not provide guidance on how to assess the information gathered and how to collect it in a manner consistent with privacy-related statutes and policies. See Security Executive Agent Directive 5 (SEAD-5), Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications, May 12, 2016. At https://www.dni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf. See also Marko Hakamaa, "Guidance from ODNI Needed for Use of Digital Information in Clearance Process," Clearance Jobs, February 18, 2019. At <https://www.clearancejobsblog.com/guidance-from-odni-needed-for-use-of-digital-information-in-clearance-process/>.

⁷ For additional information on the value of PAEI, see Intelligence and National Security Alliance, *The Use of Publicly Available Electronic Information for Insider Threat Monitoring*, February 2019. At <https://www.insaonline.org/wp-content/uploads/2019/02/FINAL-PAEI-whitepaper.pdf>.

In sum, all cleared contracting firms have automated processes in place to continually monitor and evaluate their employees' behavior, including social media activity, through their insider threat programs. In contrast, only some agencies have instituted such monitoring through CE programs, and no government CE programs currently monitor federal employees' social media activity. As a result, more contractors are subject to comprehensive continuous monitoring than federal employees, and only contractors have their social media monitored for concerning statements and activities.

Information Sharing on Personnel Risks Is One-Way

Information sharing is crucial when trying to identify insider threats. Aberrant or potentially risky behavior must be reported to someone – employers, clients, co-workers, supervisors –who can investigate, assess, and ultimately mitigate any potential risk. As Figure 2 illustrates, the more information that is shared, the lower the risk that potentially dangerous behavior goes undetected.

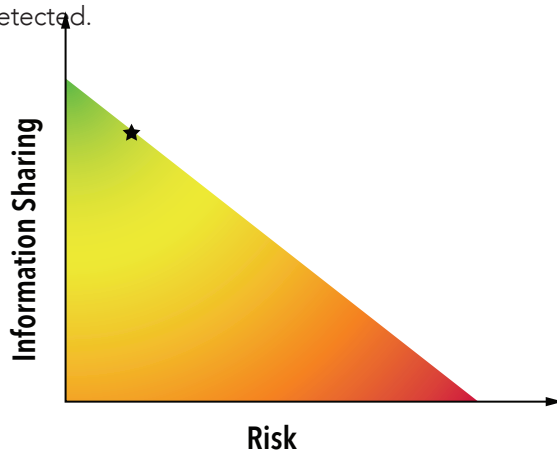


Figure 2: Relationship between information sharing and risk

The challenge, however, is that when a contractor is assigned to a federal agency work site, company supervisors have less than fulsome insight into the person's behavior, and federal employees who are co-located with the person have little incentive or ability to act upon concerning behavior that they notice. As a result, information on concerning behavior could go unnoticed by company executives or unreported by agency officials.

Contractor Sharing with Government

Information sharing regarding potential employee misconduct is generally a one-way street. Contractors are required by Government industrial security policy, as outlined in NISPOM,⁸ to report adverse and insider threat information regarding their employees, including mishandling of classified information, foreign contacts and travel, and information about an employee's financial situation, personal conduct, reliance on drugs or alcohol, criminal convictions, and other information that raises doubt about the employee's character, judgment, or reliability.⁹

However, once an individual contractor is hired, granted a security clearance, placed on a government contract, and assigned to a government facility, the contracting firm has little insight into its employee's day-to-day behavior. Moreover, the intangible behavioral habits of an employee, which could be indicators of personal or professional stress, are not observable by the company. With no way of knowing that its employee may be struggling, the company has no way of intervening to assist its employee or remove him/her from a position where he/she could cause harm. INSA recommends that companies should train supervisors to manage off-site employees with an eye to monitoring their professional behavior and general well-being. Although firms could develop such training individually, it may make sense for them to collaborate so as to identify best management and risk mitigation practices.

⁸ Department of Defense, National Industrial Security Program Operating Manual (Incorporating Change 2), DoD 5220.22-M, Updated May 18, 2016. At <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf>.

⁹ See Center for Development of Security Excellence (CDSE), NISPOM Reporting Requirements, no date. At https://www.cdse.edu/documents/cdse/CDSE_RR_JobAid.pdf.

Unfortunately, federal officials often have little opportunity to intervene if they notice a contractor exhibiting behavior of concern. From the perspective of a government agency, contractors are not “our employees”; as a result, agency human resources professionals cannot offer services, counseling, or training to a contract employee who may appear to be in distress. Government co-workers may not notice changes in the contractor’s behavior, as they may not interact directly with contractor colleagues as frequently or as in-depth as with their civil service co-workers. Government project managers may not have access to previous or current performance evaluations to assess whether a contract employee’s work quality and habits have deteriorated compared to previous work.

Complicating matters, the FAR and Defense Federal Acquisition Regulation Supplement (DFARS) conflict with the Privacy Act regarding sharing of data; the DFARS addresses the sharing of information from industry to government, while the Privacy Act addresses government to industry.

The DFARS (specifically Section Subpart 204.73—Safeguarding Covered Defense Information and Cyber Incident Reporting) states, “Contractors and subcontractors are required to rapidly report cyber incidents directly to DoD.”¹⁰ However, no reciprocal policy exists that requires DoD to share information with contractors.

“The DFARS states, “Contractors and subcontractors are required to rapidly report cyber incidents directly to DoD.” However, no reciprocal policy exists that requires DoD to share information with contractors.

Government Sharing with Contractors

Although companies are required to share derogatory information with their government clients, government agencies do not tell contracting firms when they have identified similarly concerning behavior related to the contractor’s employees. Interviewees asserted that the reasons for government’s inability or refusal to share information stem from agencies’ differing – and sometimes overly cautious – interpretations of privacy laws. Some agencies, according to interviewees, believe the Privacy Act of 1974¹¹ and other statutes prevent them from telling a contract worker’s employer about behavioral red flags. As a result, when an individual contractor commits a security violation or otherwise comes under scrutiny, that individual’s employing company is generally not told that its employee poses security concerns. In the absence of such reporting, the worker’s firm may assign him/her to another agency, where the risk posed by the worker would persist.

¹⁰ Department of Defense, *Defense Federal Acquisition Regulation Supplement (DFARS), Sec. 204.7302(b)*. At https://www.acq.osd.mil/dpap/dars/dfars/pdf/current/20190809/204_73.pdf.

¹¹ *Privacy Act of 1974*, 5 U.S.C. § 552a.

Technically, to report a problem with a contract employee, a government project manager must first inform the Contracting Officer Technical Representative (COTR) overseeing the contract, not the employee or the employee's corporate supervisor. The absence of direct lines of communication that enable discussions of concerning behaviors by the people directly involved often prevents such behaviors from being addressed.

Alerts would then be generated if a person accessed sensitive materials they had no need to see, misused computer networks, mishandled classified documents, or showed indicators of potential workplace violence. The Defense Department's Joint Personnel Adjudication System (JPAS) captures these red flags – when they are reported to security and then entered into the system – but the Defense Counterintelligence and Security Agency's (DCSA's) Joint Verification System (JVS) does not. However, companies can't see alerts in these systems, and so cannot take corrective actions.

If personnel security risks are to be mitigated effectively, government agencies must provide employers with sufficient information for the employing firm to mitigate the risk through counseling, ongoing monitoring, and/or termination. If such information sharing requires changes to statute or policy, the Intelligence Community should pursue such changes.

To close these gaps in security policy, government agencies must agree upon a uniform interpretation of privacy laws that treats contractors who hold government-issued security clearances in the same way as cleared government employees. The Security Executive Agent (SecEA), in conjunction with the Department of Justice (DOJ), should clarify these requirements so agencies can take steps to mitigate security risks. If the SecEA and DOJ determine that statutory changes are required to enable government to notify firms of risks posed by their employees, the Administration should propose language to Congress that would rectify this critical shortcoming. Separately, the DFARS should be revised to allow for greater sharing of information from industry to government.

“When an individual contractor commits a security violation or otherwise comes under scrutiny, that individual's employing company is generally not told that its employee poses security concerns.”

To illustrate, Figure 3 shows the security clearance life cycle. In practice, while contractors share information about at-risk employees with government (green arrow below), the government is unwilling to share this information with industry (blue arrow above).

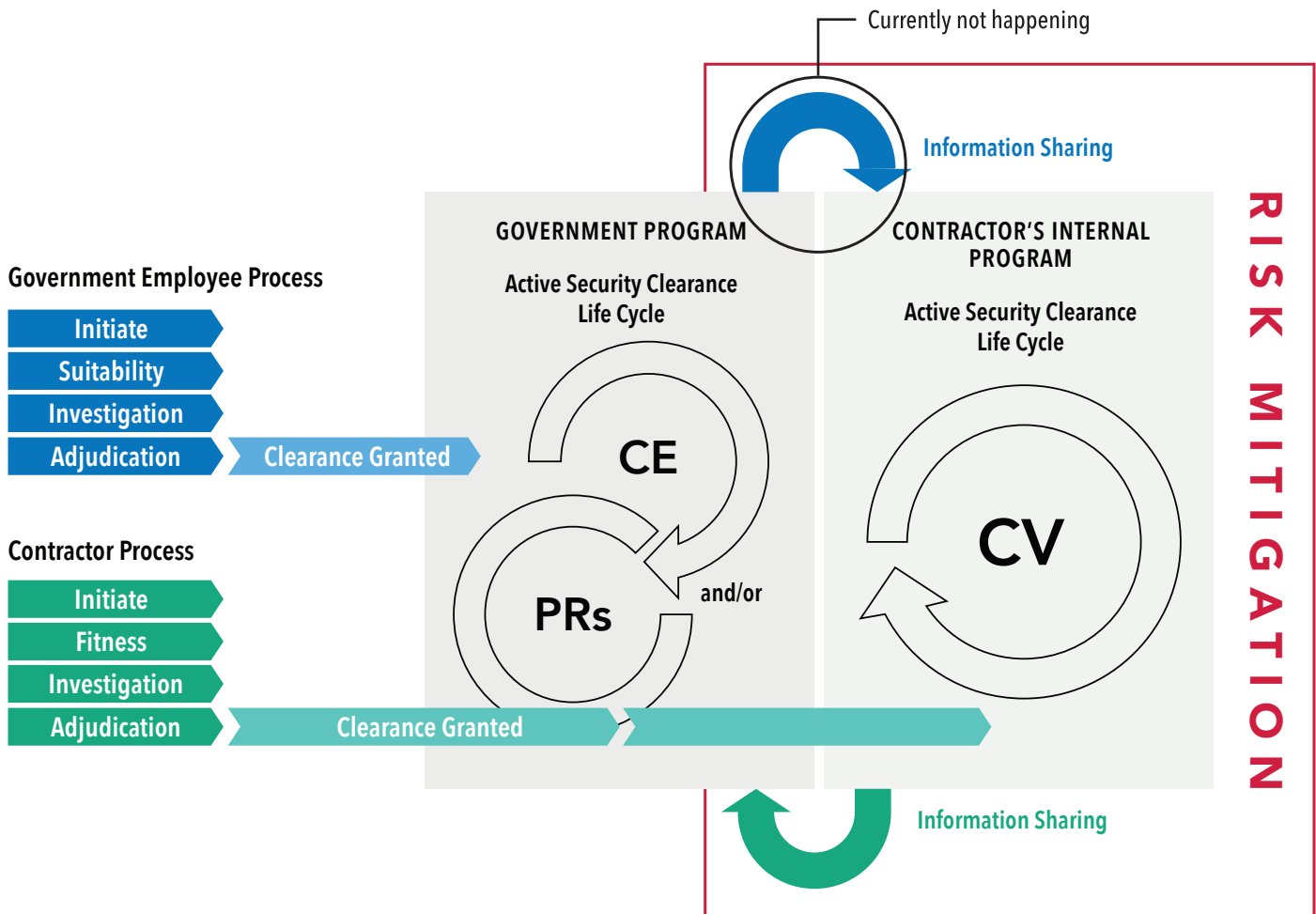



Figure 3: Mitigating Risks through Corporate CE Programs and Information Sharing

Government Often Fails to Track Derogatory Data Across Contracts

Another significant difference identified in interviews is that government agencies do not always capture comprehensive information on contractors who have worked for multiple private companies. Critical derogatory information that could sway an adjudication, such as security violations, are often unrecorded – especially if the employee quits before an investigation into allegations of misbehavior have been completed. Additionally, once an employee leaves a company, the company is no longer obligated by the NISPOM to report the misbehavior to the Defense Counterintelligence and Security Agency (DCSA), which means the derogatory findings may never be entered into the employee’s JPAS or Scattered Castles (SC) security file.¹² Thus, a contractor’s bad conduct does not follow them as they move from one job to the next in the corporate world. With government employees, one can find a more complete record of actions in official human resources records; government employees do not typically change employers as frequently, so reports of adverse actions are typically available when they do so.

Although agencies reserve the right to refuse the services of any contractor or applicant who is judged to be a security risk, the government is not permitted to provide details of its reasoning as a result of Privacy Act restrictions. When the government doesn’t explain why it refused an individual contractor, the employing company has no cause to fire the person. Thus, the company could still place the employee on another contract in another department or agency.



When the government doesn’t explain why it refused an individual contractor, the employing company has no cause to fire the person. Thus, the company could still place the employee on another contract in another department or agency.

In addition, a determination by an agency that a person is not suitable to perform work under a contract is not a denial, suspension, or revocation of a previously granted security clearance by another agency. As a result, one agency’s decision that a contractor poses an undue risk does not necessarily lead to the revocation of the person’s clearance.

¹² The Defense Department’s Joint Personnel Adjudication System (JPAS) at least captures red flags – when they are reported to security and then entered into the system, which is not always the case. However, the Defense Security Service’s Joint Verification System (JVS) – a component of the Defense Department’s System of Record for comprehensive personnel security, suitability, and credential management for all DOD personnel – does not.

RECOMMENDATIONS

INSA makes the following recommendations to promote greater information-sharing between government and industry:

- The DNI, as the government's Security Executive Agent, in coordination with the Department of Justice and all agencies doing classified work, should coordinate the development of a uniform, government-wide interpretation of what information can be shared under the Privacy Act. If this effort determines that changes to the Privacy Act are required to effectively mitigate security risks, the White House should propose whatever statutory changes are needed.
- The DNI, as Security Executive Agent, should continue efforts to implement Continuous Evaluation programs across the entire government for all cleared federal employees and contractors.
- The Defense Department should amend the DFARS to allow government to share information with industry about employee behavior or actions that indicate a risk of an insider threat. The Privacy Act contains language that allows the government to report on *government* employees who pose a risk or for security clearance purposes, so government should similarly be permitted to report on *industry* employees to industry. Revisions to the DFARS could permit such sharing.
- Agencies should enter all derogatory information into JPAS and SC so it is available when contractors change jobs. INSA recommends that all clearance/ access denials or terminations should be reported in JPAS and SC with explanations of why the contractor employee's services were denied or terminated. It should then be required that the JPAS/SC files of all contractors being assigned to work on any government contract – for any agency – shall be reviewed for security risks.
- DCSA should clarify NISPOM requirements regarding reporting of security incidents. Although the NISPOM sets thresholds for reporting security incidents, many contractors we interviewed reported a lack of clarity regarding the types of incidents that need to be reported. Among other changes, the NISPOM should make clear that contractors should be required to report the departure or termination of an employee due to a security incident.
- Government Agencies must agree upon a single common standard regarding the use of publicly available electronic information, specifically social media, for personnel security and insider threat purposes. The DNI, as Security Executive Agent for the government, must then develop guidelines for the implementation of this standard throughout the sector.
- Industry should be required to provide the government a standard set of suitability information on employees that is equivalent to the information acquired for government employees.
- Companies should train supervisors to manage offsite employees with an eye to monitoring their status and well-being. As noted, contractors who work at a government location – especially when no co-worker or supervisor is co-located with them – are subject to limited oversight by their employing firm. Although firms could develop such training individually, it may make sense for them to collaborate so as to identify best management and risk mitigation practices.

ACKNOWLEDGEMENTS

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

INSA MEMBERS

Sandy Maclsaac, *Deloitte; Subcommittee Chair*

Vinny Corsi, *IBM; Subcommittee Vice Chair*

Julie Coonce, *TransUnion*

Michael Hudson, *Clearforce*

Joseph Kraus, *ManTech*

David Luckey, *RAND Corporation*

Kathy Pherson, *Pherson Associates*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

Chuck Alsup, *Former President*

Larry Hanauer, *Vice President for Policy*

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

Caroline Henry, *Marketing & Communications Assistant*

Jessica Willmore, *Intern*

Megan Anderson, *Intern*

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 INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies (particularly, but not only, those working on intelligence and national security issues), cleared contractors, and other public and private sector organizations. The objective of the Subcommittee's work is to enhance the effectiveness, efficiency, and security of both government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.



INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Building a Stronger Intelligence Community

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