



INTELLIGENCE AND  
NATIONAL SECURITY  
ALLIANCE



OCTOBER 2021

# The Need for Transparency on Insider Threats:

## *Improving Information Sharing Between Government and Industry*

*Presented by*  
INSA'S INSIDER THREAT SUBCOMMITTEE

*Building a Stronger Intelligence Community*

## EXECUTIVE SUMMARY

Cleared government contractors need insight into their employees' behavior to successfully identify, evaluate, and mitigate security threats and implement government-mandated insider threat programs.<sup>1</sup> However, when their employees work on-site at government facilities, only the government agency being supported is positioned to detect conduct indicative of a security risk – for example, downloading classified files unrelated to one's job or threatening to harm co-workers. In most cases, however, government agencies do not tell the employing firm that their staff member may pose security risks, making it impossible for the company to mitigate potential threats. This lack of transparency is driven by a misunderstanding of the law – particularly the Privacy Act of 1974 – and a lack of clear policy guidance.

New legislation and policies are needed to enable all government agencies to share appropriate personnel security information and thereby mitigate security risks already known to the government. INSA recommends that the executive branch clarify an appropriate level of information that can be shared under the law, issue clear policy guidance directing maximum transparency, and streamline information-sharing procedures. INSA also recommends that Congress pass Section 502 of the Senate's FY2022 Intelligence Authorization bill [S. 2610], which would require agencies to share observed security-relevant information on contractor employees with the employing firms.

<sup>1</sup>The National Insider Threat Task Force (NITTF), part of the Office of the Director of National Intelligence (ODNI), defines an insider threat as "a threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, their authorized access to any U.S. Government resource." See *National Insider Threat Task Force Mission Fact Sheet*, no date, at [https://www.dni.gov/files/NCSC/documents/products/National\\_Insider\\_Threat\\_Task\\_Force\\_Fact\\_Sheet.pdf](https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf). INSA's Insider Threat Subcommittee defines the threat more broadly to include trusted individuals who use their authorized access to cause harm to a government agency or company. INSA's definition also encompasses threats of workplace violence. For details, see INSA, "Explanation of INSA-Developed Insider Threat Definition," November 2015. At [https://www.insaonline.org/wp-content/uploads/2018/10/INSA\\_InsiderThreat\\_definition-Flyer.pdf](https://www.insaonline.org/wp-content/uploads/2018/10/INSA_InsiderThreat_definition-Flyer.pdf).

## INTRODUCTION

U.S. defense and intelligence agencies collaborate extensively with cleared contractors<sup>2</sup> to secure capabilities and resources that they do not possess in-house. Government agencies have insights into the behavior of cleared contractor employees who work on government computer networks at government facilities. When such individuals demonstrate behavior that indicates a potential security risk, agencies generally fail to share relevant information with the contractor firm, creating risks for the security of classified information, secure networks, and workplace safety. Legislation and policies requiring all government agencies to share appropriate personnel security information are needed to reduce these risks.

Security Executive Agent Directive 3 (SEAD-3) requires information to be shared in only one direction – from cleared contractors to the United States Government (USG).<sup>3</sup> No policy or statute exists to prevent government agencies from sharing information with contractors; however, government officials are often reluctant to share details about suspicious behavior by a contractor's employees with the contractor.

To address this situation expeditiously and thereby mitigate risk more effectively, the Intelligence and National Security Alliance (INSA) recommends a series of policy, legal, and procedural solutions that will require close coordination among stakeholders across government and industry.

“

The lack of clear policy guidance on what personnel security information USG agencies can share with cleared contractors has created confusion and uncertainty and prevented uniform and consistent security practices across industry.

## BACKGROUND

Under the National Industrial Security Program (NISP), the USG requires cleared contractors and cleared contractor employees to protect classified information in a manner equivalent to those procedures used by executive branch agencies. The National Industrial Security Program Operating Manual (NISPOM) and several other USG policies and regulations specify compliance standards for cleared contractors to ensure uniformity and consistency within industry. Among the NISPOM's standards is the requirement for all cleared contractors to implement comprehensive insider threat programs. Such initiatives depend upon information from multiple sources, including supervisors, co-workers, and computer network user activity monitoring (UAM). When a contractor employee works on-site at a government facility, it is the government agency being supported – not the company employing the individual – that has access to the information and insights on the employee's daily work activities. Cleared contractors need this information about their employee's behavior for their insider threat programs to identify, evaluate, and mitigate security threats successfully.

<sup>2</sup>Throughout this paper, the term “cleared contractor” refers to a corporate entity, either for-profit or not for-profit, which has a contractual relationship with the government to perform classified work that requires its employees to hold security clearances. The cleared employees of such entities will be referred to as “cleared contractor employees.”

<sup>3</sup>Office of the Director of National Intelligence, “Security Executive Agent Directive 3 (SEAD 3): Reporting Requirements for Personnel with Access to Classified Information of Who Hold a Sensitive Position,” June 12, 2017. At <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf>.

While personnel security initiatives focus principally on identifying and mitigating threats to sensitive and classified information, such initiatives must evolve, to include information that may indicate whether a person may harm themselves or others. This physical security focus is meant to prevent incidents like the 2013 Washington Navy Yard shooting, in which a cleared contractor employee killed twelve people.

The lack of clear policy guidance on what personnel security information USG agencies can share with cleared contractors has created confusion and uncertainty and prevented uniform and consistent security practices across industry. New policies, and potentially new legislation, are needed to ensure uniform and consistent sharing of personnel security information from USG agencies to cleared contractors.

The President directed the Office of Management and Budget (OMB) to lead an interagency review of suitability and security clearance procedures for Federal employees and contractors following the Navy Yard shooting. That review underscored the critical importance of uniform and consistent information sharing.<sup>4</sup> It assessed USG policies, programs, processes, and procedures involving determinations of federal employee suitability, contractor fitness, and personnel security. The interagency working group

also evaluated the collection, sharing, processing, and storage of information used to make suitability, credentialing, and security decisions. It identified a need for better information sharing and consistent application of standards and policies in the security clearance procedures for both Federal employees and cleared contractor employees.



While several subsequent initiatives and measures have enhanced the capability of the USG to collect information and share it more consistently across the Federal government, those efforts do not directly address the disparity in sharing information with cleared contractors. SEAD-3 requires cleared contractors to report personnel security risks to USG agencies, but it does not require agencies to share insights on individual contractors with the firms that employ them. USG security personnel may discuss potential red flags

with individual cleared contractor employees to gather additional information and identify potentially false alerts; however, agencies' failure to share their concerns with contracting firms prevents companies from assisting in the evaluation of potential security risks posed by their own staff members.

Government agencies withhold suspicious information about cleared contractor employees due to four principal concerns.

<sup>4</sup>Office of Management and Budget, *Suitability and Security Clearance Performance Accountability Council, Suitability and Security Processes Review Report to the President*, February 2014. At <https://www.archives.gov/files/isoo/oversight-groups/nisp/2014-suitability-and-processes-report.pdf>.



## **CONCERN #1: Sharing derogatory information would violate the Privacy Act of 1974.**

USG officials often interpret the Privacy Act of 1974 as preventing the sharing of personnel security information regarding cleared contractor employees with their employers – particularly in the absence of explicit consent by the individuals concerned. However, this interpretation is mistaken.

Benjamin Powell, former General Counsel for the Office of the Director of National Intelligence (ODNI), has emphasized that the law is commonly misinterpreted. In an April 2019 paper entitled, *The Privacy Act and Information Sharing for Insider Threat Programs*, Powell wrote:

Despite commonplace claims to the contrary, the Privacy Act does not bar the sharing of this kind of information with cleared contractors. The Act contains explicit exceptions that allow the government to make disclosures in several circumstances, including disclosures to cleared contractors.<sup>5</sup>

Multiple speakers reiterated these points at a panel discussion on “Government-Industry Personnel Security Information Sharing Under the Privacy Act” held by INSA in January 2020. The panelists – who included a former ODNI General Counsel (Powell), CIA’s Privacy and Civil Liberties Counsel, a Senate Intelligence Committee staff member, and the Director of the Defense Department’s Office of Hearings and Appeals (DOHA) – argued that obstacles to sharing personnel security information on cleared contractor employees are rooted in policy, not in the Privacy Act.<sup>6</sup>

To eliminate the widely held belief that the Privacy Act prevents such information sharing, INSA’s Insider Threat Subcommittee recommended in a January 2020 white paper that ODNI and OMB convene an interagency legal working group so “government lawyers [can] agree upon a uniform, government-wide interpretation of what information can be shared with industry under the Privacy Act” and related legislation.<sup>7</sup> If statutory changes are needed to share information that could mitigate security threats, INSA recommended, OMB should propose changes to Congress that would explicitly allow insider threat information to be shared with cleared contractors.

Congress took steps on its own to address privacy concerns in a provision of the Fiscal Year 2020 National Defense Authorization Act calling for enhanced two-way information sharing. Section 6610(f) of the law called for the Federal government’s Security Executive Agent (the Director of National Intelligence) and its Suitability and Credentialing Executive Agent (the Director of the Office of Personnel Management) to consider expanding the sharing of information held by the Federal Government related to contract personnel with the security office of the employers of those contractor personnel. The statute specifically directed that the plan include mechanisms to address privacy concerns.<sup>8</sup> Unfortunately, this concept was never put into practice, as the statute merely called for these officials to develop a plan to implement a pilot program to assess the feasibility and advisability of sharing this information. Solving the problem requires more than a plan for a pilot to assess the merits of transparency.

<sup>5</sup>Benjamin Powell, “The Privacy Act and Information Sharing for Insider Threat Programs,” white paper, Wilmer Hale, April 2019. At <https://www.insaonline.org/wp-content/uploads/2021/09/Privacy-Act-White-Paper.pdf>.

<sup>6</sup>Intelligence and National Security Alliance, *2020 National Security Legal Outlook*, event description, January 16, 2020. At <https://www.insaonline.org/event/2020-national-security-legal-outlook/>.

<sup>7</sup>Intelligence and National Security Alliance, *Legal Hurdles to Insider Threat Information Sharing*, January 2020, pp. 8-9. At [https://www.insaonline.org/wp-content/uploads/2020/01/INSA\\_WP\\_Legal-Hurdles\\_FIN.pdf](https://www.insaonline.org/wp-content/uploads/2020/01/INSA_WP_Legal-Hurdles_FIN.pdf).

<sup>8</sup>National Defense Authorization Act For Fiscal Year 2020, P.L. 116-92, 116th cong., 1st sess., section 6610(f). At <https://www.congress.gov/116/crpt/hrpt333/CRPT-116hrpt333.pdf>.

The following year, the Senate called for more direct action in Section 403 of its FY 2021 Intelligence Authorization bill (S. 3905).<sup>9</sup> This provision called for the Director of National Intelligence (DNI), as the Federal government's Security Executive Agent (SecEA), to issue a policy requiring agencies to share suspicious behavioral information pertaining to contractor employees with that person's employing firm. The draft legislation explicitly addressed concerns that such information could be used to the detriment of innocent contractor employees:

- It addressed employee consent to information-sharing by requiring contractor employees to agree to such sharing as a condition of receiving a security clearance.
- It ensured information would not be misused by requiring contractors to use the information exclusively for insider threat risk mitigation.
- It specified that contractor employees have the right to challenge the derogatory information and remedy any security concerns.
- It prevented contractor security officials from discussing the derogatory information with other parties, thereby preventing personnel action (such as termination) not linked to risk mitigation.

While the Senate incorporated S. 3905 into the National Defense Authorization Act for FY2021 in the last days of the 116th Congress, this provision – which would have rectified the problem – was removed from the final legislation.<sup>10</sup> Congress is reconsidering this provision in the 117<sup>th</sup> Congress, however; the Senate Select Committee on Intelligence (SSCI) included identical language in section 502 of its markup of the Fiscal Year 2022 Intelligence Authorization Act (S. 2610), which it passed on a bipartisan 16-0 vote on July 28, 2021.<sup>11</sup>

## CONCERN #2:

### **Sharing derogatory information would place cleared contractor employees at risk of adverse actions by their employer before completion of fact-finding and adjudicative actions by the USG.**

As required by the NISPOM and regulations codified in the Federal Register,<sup>12</sup> cleared contractors have established insider threat programs to deter, detect, and mitigate vulnerabilities and threats from trusted insiders. **To enable cleared contractors to implement mandatory insider threat programs effectively, USG agencies should provide information developed from their own monitoring efforts so companies can intervene with employees before they become an insider threat.**

Providing personnel information to industry insider threat program managers does not increase the risk that a cleared contractor will punish its employee before completion of fact-finding. In fact, these programs are required to employ personnel specifically trained in procedures for conducting insider threat response actions; applicable laws and regulations regarding the gathering, integration, safeguarding, and use of records and data; the consequences of misuse of such information; and applicable legal, civil liberties, and privacy policies. Legislation like Section 502 of the Senate's FY2022 Intelligence Authorization bill would create further employee protections by preventing contractor security officials from discussing the information with other parties, thereby preventing personnel action (such as termination) not linked to risk mitigation. In lieu of legislation, the SecEA could also institute such protections in policy guidance.

<sup>9</sup>Intelligence Authorization Act for Fiscal Year 2021, U.S. Senate, 116th Cong., 2nd sess., S. 3905 (2020), section 403. See <https://www.intelligence.senate.gov/legislation/intelligence-authorization-act-fiscal-year-2021-reported-june-8-2020>.

<sup>10</sup>The text of the Intelligence Authorization Act (not including the provision on information-sharing) was incorporated into the National Defense Authorization Act for Fiscal Year 2021, Public Law No: 116-283, 116th Cong., 2nd sess., January 1, 2021. At <https://www.congress.gov/bills/116/congress/house-bill/6395>.

<sup>11</sup>Intelligence Authorization Act for Fiscal Year 2022, U.S. Senate, 117th cong., 1st sess., S. 3610 (2021), section 502. At <https://www.congress.gov/117/bills/s/2610/BILLS-117s2610pcs.pdf>. See also Office of Sen. Mark Warner, "Senate Intelligence Committee Passes the FY22 Intelligence Authorization Act," press release, July 28, 2021. At <https://www.warner.senate.gov/public/index.cfm/2021/7/senate-intelligence-committee-passes-the-fy22-intelligence-authorization-act>.

<sup>12</sup>See 32 CFR part 117.

**CONCERN #3:**

**Sharing derogatory information would expose the USG and/or cleared contractors to lawsuits from contractor employees who feel they had been unduly punished as a result of premature risk reports.**

Another liability concern is the perception that more robust information sharing would blur the lines between employment decisions by cleared contractors and government decision-making regarding security clearances. Without access to the underlying facts to inform its own processes and decisions, cleared contractors may infer that an adverse security clearance decision necessitates adverse employment actions. Alternatively, making no decision because of a lack of information could lead the contractor to be in violation of its responsibility to notify the Defense Counterintelligence and Security Agency (DCSA) of events that “impact the status of an employee’s personnel security clearance (PCL); may indicate the employee poses an insider threat; affect proper safeguarding of classified information; or that indicate classified information has been lost or stolen.”<sup>13</sup> Cleared contractors need information from the government to make informed decisions on how to mitigate insider threats and comply with government security policies.

Some caselaw exists regarding information sharing under NISPOM requirements. In *Becker v. Philco*,<sup>14</sup> the U.S. Court of Appeals for the 4th Circuit held that a cleared contractor is not liable for defamation of an employee because of reports made to the Government pursuant to government-created contractual requirements.<sup>15</sup> Cleared contractors may inform the government of information regarding cleared contractor employees that indicate potential security risks if there is a government requirement for that reporting. Similarly, a legislated requirement for the government to share information within these same guidelines could extend that protection to government actions.

**CONCERN #4:**

**Sharing derogatory information could result in litigation that exposes protected USG sources and methods through the legal discovery process.**

The final concern, potential exposure of sensitive information or sources due to any resulting litigation, can be managed by ensuring information and subsequent actions are based upon clear and defensible facts. Much of this information is already subject to disclosure to the cleared contractor employee who is the subject of an adjudicated clearance determination.<sup>16</sup> Thus, the information would be accessible in litigation regardless of whether the contractor is also provided with access to such information.



Cleared contractors need information from the government to make informed decisions on how to mitigate insider threats and comply with government security policies.

<sup>13</sup>National Industrial Security Program Operation Manual (NISPOM), Change 2, DoD 5220.22-M, section 1-300, updated May 18, 2016. At <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf>.

<sup>14</sup>*Becker v. Philco*, 372 F.2d 771 (4th Cir. 1967).

<sup>15</sup>The NISPOM did not exist at the time *Becker* was decided; however, the U.S. Government has interpreted the reasoning and the contractual relationship in that case to equate to the NISPOM reporting requirements.

<sup>16</sup>Intelligence Community Policy Guidance (ICPG) 704.3, section D.1, allows for the disclosure of all information used to form the basis for denial or revocation of access, including a comprehensive written explanation, the right to counsel, and the right to any documents, records and reports upon which a denial or revocation is based. See Office of the Director of National Intelligence, Intelligence Community Policy Guidance Number 704.3: Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes, October 2, 2008. At [https://www.dni.gov/files/documents/ICPG/icpg\\_704\\_3.pdf](https://www.dni.gov/files/documents/ICPG/icpg_704_3.pdf).



## RECOMMENDATIONS

INSA recommends policy and statutory changes that create greater certainty regarding the conditions in which certain types of insider threat information can be shared with cleared contractor employees and the companies that employ them. INSA also recommends that the USG modify information-sharing procedures to promote the transparency needed to mitigate security risks while alleviating employee concerns that such information could be misused. Balance can be struck most effectively if government agencies share the details of a contractor employee's concerning behavior or comments – particularly those that have been investigated, substantiated, and found to be credible – without offering subjective analysis or interpretation of such facts. REDACTED



## POLICY AND STATUTORY RECOMMENDATIONS

### 1. CLARIFY WHAT INFORMATION CAN BE SHARED UNDER THE LAW.

As INSA's Insider Threat Subcommittee recommended in its January 2020 white paper, ODNI and OMB should convene an interagency legal working group charged with developing a uniform, government-wide interpretation of what information can be shared with industry under the Privacy Act and related legislation. Such a working group could be convened under the auspices of the Federal Privacy Council, which was established in 2016 by executive order "as the principal interagency forum to improve the Government privacy practices of agencies and entities acting on their behalf"; members of the Council, which is chaired by OMB's Deputy Director for Management, include the senior privacy officials from ODNI, DOD, and other agencies that engage cleared government and contractor staff.<sup>17</sup> If the working group determines that statutory changes are needed to share information that could mitigate security threats, OMB should propose changes to Congress that would explicitly allow insider threat information to be shared with cleared contractors.

### 2. ISSUE CLEAR POLICY GUIDANCE DIRECTING MAXIMUM TRANSPARENCY.

Once the interagency legal working group develops a legal framework, the DNI, as the SecEA, should convene an interagency policy working group to develop information-sharing policy guidance affecting cleared government and contractor personnel. This directive should clarify that within the specified legal parameters, agencies' default approach should be to share as much information as possible, as maximum transparency is needed to enable companies to implement the NISPOM-mandated insider threat programs designed to reduce national security risks.

### 3. PASS SECTION 502 OF THE SENATE'S FY2022 INTELLIGENCE AUTHORIZATION BILL [S. 2610].

The draft legislation requires agencies to share suspicious information on contractor employees so their companies could effectively implement government-mandated insider threat programs while simultaneously preventing such information from being used to the detriment of contractor employees determined to pose no security risk.



INSA also recommends that the USG modify information-sharing procedures to promote the transparency needed to mitigate security risks while alleviating employee concerns that such information could be misused.

<sup>17</sup>See *Establishment of the Federal Privacy Council*, E.O. 13719, 81 Fed. Reg. 29 (February 12, 2016). At <https://www.govinfo.gov/content/pkg/FR-2016-02-12/pdf/2016-03141.pdf>.

#### 4. STREAMLINE INFORMATION-SHARING PROCEDURES

Government agencies and cleared contractors alike want to base security decisions on vetted and validated information, not rumors or isolated pieces of data. Furthermore, relying on validated data insulates agencies from accusations that their security decisions are intended to yield punitive personnel actions. Agencies could share information with contractors in two ways, with sharing of unverified information reserved for situations where potential risks are higher.

**a. Option I: Sharing Adjudicated Information of Current Cleared Contractor Employees.**

The USG could provide the cleared contractor information derived from an adjudicative action (i.e., suspension, revocation, or denial of a security clearance) taken against its employee as a result of adjudicated security information – data that has already gone through a complete vetting and validation process and meets the burden for the USG to make a security decision. Including the cleared contractor in this process would provide two benefits. First, the cleared contractor could provide actionable information of his/her/their own to the USG to strengthen its adjudicative decision or damage assessment. Second, providing validated information enables the cleared contractor to take their own mitigation measures. If the cleared contractor were to be kept in the dark about the risk its employee poses, the company would have to make an uninformed assessment about whether the person is suitable for other USG work, thereby potentially transferring risk onto a different, unsuspecting government agency.


“

If the cleared contractor were to be kept in the dark about the risk its employee poses, the company would have to make an uninformed assessment about whether the person is suitable for other USG work, thereby potentially transferring risk onto a different, unsuspecting government agency.

- b. Option II: Sharing Enhanced Monitoring Information of Current Cleared Contractor Employees.** Often, threat intelligence will drive agencies to launch a formal assessment of an employee or contractor; such efforts typically involve enhanced monitoring to determine if security risks actually exist. Even though risk indicators have not yet been fully validated at the beginning of an assessment, the USG could nevertheless share these indicators – particularly in situations where the security risks are potentially high. This would enable the cleared contractor’s insider threat program to review its own records for information that could corroborate or assuage the government’s suspicions, ensuring a more informed adjudicative decision by the government. Such transparency would be consistent with the broader goal that insider threat programs should gather disparate sources of information to inform a “whole person” assessment.

## CONCLUSION

Government and cleared industry are partners in ensuring the protection of national security information and the safety of the national security workforce. To make this partnership work, government agencies must tell cleared contractors when they suspect that an individual contractor employee poses a potential security threat. No legal or policy barriers exist to prevent such information sharing, despite common misperceptions to this effect. To enable the fullest information sharing permitted under existing policy and legislation, the Intelligence Community must clarify what information can be shared and under what circumstances. If the Intelligence Community does not do so through clear policy guidance, Congress should mandate effective information sharing through legislation.

Cleared contractors are committed to protecting sensitive and classified information, as they are required to do under the NISPOM and under individual contracts for classified work. Indeed, failure to do so could lead companies to be disqualified from further government contracts – a potential penalty far costlier than the expense of maintaining effective security and insider threat programs. To meet their security obligations and effectively implement mandatory insider threat programs, cleared contractors need all pertinent information the government may have regarding risks posed by their employees. Concerns regarding employee privacy can be addressed by limiting the use of personnel security information to security matters and by limiting sharing to validated information, except in circumstances in which potential security risks are high. Greater transparency on insider threat matters will yield greater security for the nation. 



INTELLIGENCE AND  
NATIONAL SECURITY  
ALLIANCE

## ACKNOWLEDGEMENTS

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

### INSA MEMBERS

Vinny Corsi, *IBM; Insider Threat Subcommittee Chair*

Sue Steinke, *Peraton;  
Insider Threat Subcommittee Vice Chair*

Joshua Massey, *MITRE*

Greg Torres, *Booz Allen Hamilton*

Timothy Calhoun, *Booz Allen Hamilton*

Joseph Kraus, *ManTech*

Eric Roscoe, *SANCORP*

Gary Ross, *Bush School of Government and  
Public Service, Texas A&M University*

### INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

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

Britany Dowd,  
*Marketing and Communications Assistant*

Rachel Greenspan, *Intern*

Cassie Crotty, *Intern*

Ali Berman, *Intern*

---

## ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

---

## 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, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.