



THE USE OF PUBLICLY AVAILABLE ELECTRONIC INFORMATION FOR INSIDER THREAT MONITORING

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Insider Threat Subcommittee

January 2019



CONTENTS

01	EXECUTIVE SUMMARY	08	CONSIDERATIONS & RECOMMENDATIONS
03	BACKGROUND	08	Federal Government
05	TYPES OF PAEI & POTENTIAL VALUE	09	Private Organizations
05	Social Media	09	Recommendations
05	Information Regarding Financial Health	09	1. Ensure leadership support
06	Law Enforcement and Court Records	09	2. Define and communicate internal policies
06	Travel	10	3. Determine legal constraints
07	Civic Activity	10	4. Identify relevant information sources
07	Dark Web	10	5. Establish policies for use of PAEI
		11	6. Assess timeliness, credibility and accuracy of PAEI
		11	7. Determine how to efficiently process PAEI data
		11	8. Ensure validity of data
		11	9. Adapt to changes in data availability and evolving social mores
		12	CONCLUSIONS

INSA SUPPORTS A HEALTHY PLANET

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



EXECUTIVE SUMMARY

Publicly available electronic information (PAEI) – defined as information that is available to the public on an electronic platform such as a website, social media, or database (whether for a fee or not) – can provide insight into an individual’s perceptions, plans, intentions, associations, and actions. Proper use of PAEI can help employers examine, on a continual basis, whether an employee poses a potential threat to the organization’s information, assets, people, or facilities, as well as to themselves. Continuous evaluation of PAEI is especially valuable for assessing employees working within the growing “perimeter-less workspace” (at client locations, at home or from the road) where abnormal or atypical behavior – both in-person and on an organization’s networks – may be less visible to colleagues and managers. PAEI can also be used to initiate or provide context to an internal investigation into insider threats.

As the U.S. Government overhauls its security clearance process, it must decide what kinds of publicly available information to use and how to apply it to assess a candidate’s trustworthiness. To do so, it must determine what information constructively informs a risk assessment, what types of information are appropriate to use, and how to use such information to make both initial and ongoing assessments of the risks posed by individual employees.

The Director of National Intelligence (DNI), in his/her role as the government’s Security Executive Agent, must work with the Defense Department, which is assuming government-wide investigation and adjudication responsibilities, to develop a single legal interpretation of what PAEI may be collected and analyzed and to develop policies for how it may be used for security-related personnel determinations.¹ A government decision regarding the use of PAEI for personnel security and insider threat purposes will set the standard for the use of such information by organizations in both the public and private sectors.

¹ While PAEI is used to inform security clearance determinations, it is also used for less intrusive but more widespread public trust determinations. Public trust assessments, which are undertaken by (or under the auspices of) the U.S. Office of Personnel Management, examine whether a potential employee is suitable for a position that is sensitive or that requires a high degree of integrity but that does not require a security clearance for access to classified information. Examples include public safety and health workers, officials entrusted with financial matters, or officials with access to sensitive data or information systems. Because a large percentage of investigative resources are dedicated to public trust assessments rather than security clearances, enrolling public trust employees in continuous evaluation programs that draw on PAEI would likely enable investigative resources to be devoted to higher priority or more challenging cases. This paper, however, focuses solely on the use of PAEI for the investigation and continuous evaluation of personnel with security clearances.

The types of PAEI that could be examined are extremely varied. Some data – such as arrest and conviction records – are widely available to the public and would seem to have a direct bearing on whether someone is likely to obey laws and follow regulations in the future. Some data – such as credit reports – may be available only through commercial purchase and may have the ability to indicate, but not demonstrate, potential risk. Yet other types of information – such as personal commentaries and photos posted on social media – may require some effort to locate, correlate less directly to the degree of risk the subject poses in a workplace, and be seen by employees as inherently “private” and thus as overly intrusive for an employer to collect.

“Proper usage of PAEI can help managers identify insider threat behavior before a harmful action is taken. Indeed, refusal or failure to consult PAEI could render an organization vulnerable to avoidable risks.”

The following questions may help both public and private sector leaders determine how their organizations should use PAEI for personnel evaluations:

- Can the data can be legally collected and assessed?
- Is the organization and its leadership comfortable using the data?
- What will be the impact of using PAEI on organizational culture and employee morale? Are certain types of PAEI (such as social media posts) considered more “personal” than others (such as credit reports)?

- What internal policies must be implemented before using the data?
- What data can reliably contribute to an analysis of insider threat risks?
- What is the integrity, timeliness, and accuracy of the data?
- How can the data be efficiently processed and analyzed?

While addressing these questions, the following employee protection measures can provide confidence for organizations considering PAEI as an insider threat resource:

- PAEI collection and analysis should be governed by written policies that are clearly communicated to the workforce.
- To ensure maximum respect for employees’ privacy, only PAEI that is relevant and useful for assessing threats to the organization, its people, its information, and its facilities should be collected and analyzed.
- Except when necessary to thwart potential imminent threats, PAEI should not be the sole determinant for decision-making or action; it must be considered and analyzed in a broader context.
- Organizations should institute data validation processes to ensure that outside data is reliable and attributed to the correct employee.
- Organizations’ consideration of PAEI should evolve along with changes in social mores, legal standards, and expectations of privacy.

BACKGROUND

An insider threat is the hazard posed by an individual who may abuse his/her authorized access to information or facilities to harm an organization or its employees.² Such individuals generally (but not always) act wittingly and with malicious intent. They can inflict harm through a range of activities, such as committing espionage, leaking classified or sensitive information, sabotaging work products or computer networks, or committing acts of violence in the workplace.

Many organizations have insider threat programs that monitor employees' activities to identify risky behavior – ideally before an at-risk employee causes any damage. Proper usage of Publicly Available Electronic Information (PAEI) can help managers identify insider threat behavior before a harmful action is taken. Indeed, refusal or failure to consult PAEI could render an organization vulnerable to avoidable risks. Note that within the context of an insider threat program or investigation, PAEI encompasses information that is available to the public – whether for a fee or not – on an electronic platform such as a website, social media application, or database. It does not include data or activities within an employer's internal network, which is by its nature not publicly available and which many employers routinely assess for insider threat purposes. Once considered a desirable but optional element of insider threat programs, PAEI is now considered a critical resource.

The proliferation of digital information over the last two decades has prompted this change. The increasing use of online tools and near-omnipresent handheld devices – which, with users' consent, collect and report data on individuals' activities – has led companies to compile such information into databases that can provide detailed personal, financial, and professional profiles of almost any individual. Furthermore, dramatic technological advances have allowed instantaneous global communication through discussion forums, social media, and online publishing platforms. Younger generations, known as “digital natives” for having never lived without advanced electronic devices and the Internet, conduct much of their lives in cyberspace, tending to use social media and public forums as their first choice for self-expression. They also tend to share far more online, providing valuable insight into their perceptions, plans and intentions.

² In December 2015, INSA's Insider Threat Subcommittee developed a comprehensive definition of insider threat that was briefed to, and accepted by, the directors of the Defense Security Service (DSS) and the National Counterintelligence and Security Center in the Office of the Director of National Intelligence (ODNI/NCSC). INSA's definition is as follows: “The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.” See INSA, “Explanation of INSA-Developed Insider Threat Definition,” December 2015. At <https://www.insaonline.org/explanation-of-insa-insider-threat-definition/>.

The availability of massive governmental and commercial databases – some compiled by commercial firms for a fee, and others posted online for free – means that a wide range of information about individuals’ personal, financial, and professional behavior can be consulted easily. This data can inform security assessments in multiple ways, starting with pre-employment screening and continuing through data collection in the wake of a security incident. In between, it adds critical value to systems that continuously evaluate employees’ behavior against tripwires that could indicate malicious activity (by reflecting anomalous behavior) or by identifying antagonistic actions or acrimonious opinions that could be precursors to malicious acts.

The wide spread use of social media for personal expression and communication means people are more likely to use these outlets to voice their hostility, anger or plans for malicious or violent activity. Indeed, rather than confide in a close friend or coworker, disgruntled individuals are more likely to express themselves on these platforms, where they can find sympathetic ears and “likes” and hide behind a cloak of anonymity.

Many government employees who engaged in criminal or violent behavior had exhibited indicators of nefarious activity prior to their ultimate discovery, whether by posting anti-government or violent sentiments on social media, getting arrested, or engaging in suspicious financial activities, all of which would have been revealed in public records data. Troubled employees who tipped their hand through such behavioral indicators include NSA hoarder Harold Thomas Martin, who was arrested for drunken driving, charged with misdemeanor harassment, and had a lien placed on his house for 14 years due to unpaid taxes,³ and Washington Navy Yard shooter Aaron Alexis, who had been arrested multiple times both before and after enlisting in the Navy.⁴

Given the clear applicability of PAEI to employee background investigations and insider threat assessments, both the Department of Defense and the Intelligence Community decided to draw on PAEI for their continuous evaluation (CE) programs. However, agencies remain undecided on what PAEI sources they will use and how they will apply the information. As a result, as both DOD and the ODNI roll out their respective CE programs, the Intelligence and Defense communities are using different sources of information to make clearance determinations for employees who may work in both realms.

The use of PAEI has contributed to the reduction of an enormous backlog of security clearance cases that reached 725,000 people in June 2018.⁵ Furthermore, the incorporation of PAEI into CE programs could both reduce (or even eliminate) the need for periodic reinvestigations of employees at five- or ten-year intervals and mitigate risks by identifying potentially concerning behavior in near-real time.

As the U.S. Government reforms its security clearance process, it must address the use of PAEI – particularly employees’ social media accounts and commercially available databases – for personnel security and insider threat purposes.

³ Scott Shane and Jo Becker, “N.S.A. Appears to Have Missed ‘Big Red Flags’ in Suspect’s Behavior,” *New York Times*, October 29, 2016. At <https://www.nytimes.com/2016/10/30/us/harold-martin-nsa.html>.

⁴ Tom Vanden Brook, “Report: Concerns About Navy Yard Shooter Never Reported,” *USA Today*, March 18, 2014. At <https://www.usatoday.com/story/news/nation/2014/03/18/navy-yard-shooter-called-insider-threat/6558373/>.

⁵ Office of Management and Budget (OMB), Performance Accountability Council (PAC), “Security Clearance, Suitability/Fitness, and Credentialing Reform,” *FY2018 3rd Quarter Update*, slide 5. At https://www.performance.gov/CAP/action_plans/FY2018_Q3_Security_Suitability.pdf.

TYPES OF PAEI & POTENTIAL VALUE

SOCIAL MEDIA

Social media is the most prevalent type of PAEI, and in many cases the most telling of an individual's state of mind. A person's postings to Facebook, Twitter, Instagram, YouTube, LinkedIn, and other online publishing platforms may reflect unusually negative (and even violent) sentiments toward his or her employer, colleagues, public figures, family members and former partners. It may also reveal disturbing or even illegal behavior, such as serial drunkenness or drug use. Social media posts can also, however, reveal personal comments or behavior that are merely embarrassing and shed no light on a person's fitness for service.

Because of the wide range of personal thoughts and activities that people share on social media, many employees may consider monitoring of their social media overly intrusive. Despite the public nature of social media sites and the failure by many users to make use of available access controls, many Americans feel that their social media and broader online activity deserves some measure of privacy protection. Yet by failing to make use of available privacy settings on many social media platforms and web sites, many people make their online activities publicly visible. While a 2015 Pew poll indicated that 55 percent of Americans believe they should have the ability to use the Internet completely anonymously,⁶ an April 2018 Reuters/Ipsos poll indicated that 45 percent of Twitter users and 40 percent of Instagram users did not know what their privacy settings were.⁷

INFORMATION REGARDING FINANCIAL HEALTH

Bankruptcies, credit reports, bank data, tax reports, and similar documentation may indicate sudden changes in financial health, including unexplained affluence or financial difficulties. Excessive debt, including new or especially dire circumstances, and habits of living beyond one's means could lead a trusted employee to sell classified, sensitive, or privileged information. CIA turncoat Aldrich Ames, for example, cited money as one of his primary motivations for spying for the Soviet Union.⁸ Information on employees' finances is easily available through credit checks. Indeed, information gathered under the Fair Credit Reporting Act (FCRA) has enabled employers to gain legal access to data about an employee's fiscal health earlier than would be possible by public records alone.

⁶ Mary Madden and Lee Raine, "Americans' Attitudes About Privacy, Security and Surveillance," Pew Research Center, May 20, 2015. At <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

⁷ Chris Kahan and David Ingram, "Three-Quarters Facebook Users as Active or More Since Privacy Scandal: Reuters/Ipsos Poll," Reuters, May 6, 2018. At <https://www.reuters.com/article/us-facebook-privacy-poll/three-quarters-facebook-users-as-active-or-more-since-privacy-scandal-reuters-ipsos-poll-idUSKBN17081>.

⁸ Tim Weiner, "Why I Spied: Aldrich Ames," New York Times, July 31, 1994. At <https://www.nytimes.com/1994/07/31/magazine/why-i-spied-aldrich-ames.html>.

LAW ENFORCEMENT AND COURT RECORDS

Documented insider threat incidents suggest a person does not decide to commit a crime at work overnight; rather, indicators frequently mount leading up to the incident. Law enforcement and court records can bring such turmoil in an employee's life to light. Investigations, arrests, convictions, civil suits, and protective orders may indicate unpredictability, volatility, strained personal relations, addiction, and/or an inability to follow laws and established procedures. Law enforcement involvement in an employee's life can also reflect drug, alcohol, sexual and psychological problems. When viewed in the aggregate, independent events may indicate the employee needs help and/or to be removed from a position of trust.

Unfortunately, police and court records are not universally available, nor are they consistent nationwide. Such data is stored by a wide range of law enforcement and judicial information entities at the federal, state, municipal, and tribal levels, each of which has different standards for compiling, reporting, and disseminating their records. Some jurisdictions update their data more frequently than others, making it possible to develop an overconfidence that electronic data used by CE programs is always current and up to date. The CE methodologies employed by the Intelligence Community and Defense Department must account for the disparity in the availability and timeliness of law enforcement data.

TRAVEL

Travel information, particularly undisclosed visits to foreign countries, is extremely pertinent to insider threat investigations. Individuals who commit espionage on behalf of foreign governments often travel outside of the U.S. clandestinely or without reporting it, either to receive instructions or training or to deliver sensitive information. DIA analyst Ana Montes, who spied for Cuba, repeatedly traveled clandestinely to Cuba.⁹ Aldrich Ames met his Soviet handlers in Bogota, Caracas, and Vienna,¹⁰ and State Department diplomat Felix Bloch met with his Soviet handlers in Paris, Brussels, and Vienna (often while on official travel).¹¹ Chinese security services routinely invite private sector experts in sensitive technologies to meetings or conferences in China, at which they solicit proprietary information and attempt to recruit the visitors as spies.¹²

Federal government employees and contractors with security clearances are required to report foreign travel; such reports are used to identify unusual patterns of behavior and to assess the significance of travel that is discovered despite employees' failure to report it. Private companies could impose similar requirements on personnel with access to sensitive data to identify employees who may be collaborating with foreign governments or competitors. Although records of travel may not be publicly available, individuals may make references to unreported travel or to their overseas activities on social media, on blogs, and in other public fora. Similarly, if an employee makes a presentation at a conference without seeking prior approval, the agenda for the conference may nevertheless be posted publicly on the event's web site and thus be available to the organization's security team.

⁹ Brian Latell, "New Revelations About Cuban spy Ana Montes," *Miami Herald*, August 2, 2014. At <https://www.miamiherald.com/opinion/issues-ideas/article1978099.html>.

¹⁰ Select Committee on Intelligence, U.S. Senate, *An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence*, November 1, 1994. At https://fas.org/irp/congress/1994_rpt/ssci_ames.htm.

¹¹ David Wise, "The Felix Bloch Affair," *New York Times*, May 13, 1990. At <https://www.nytimes.com/1990/05/13/magazine/the-felix-bloch-affair.html>.

¹² Michael Balsamo and Angie Wang, "Feds: Chinese spy tried to steal US aviation trade secrets," *Associated Press*, October 10, 2018. At <http://www.startribune.com/feds-chinese-spy-tried-to-steal-us-aviation-trade-secrets/496661981/>.

CIVIC ACTIVITY

An individual's in-person and online social activity can provide indications about their values and public activities. Association with persons or groups that are under investigation or are themselves considered threats may indicate a desire to cause harm. Such groups may include (but are not limited to) violent extremist organizations (whether foreign or domestic), organizations with an anti-U.S. ideology, and publishers of classified information, such as WikiLeaks. While many of these activities may be protected from criminal prosecution under the First Amendment, the Constitution does not forbid employers from deciding that such activities are inconsistent with their organization's values. Publicly stated views indicating an individual may harm themselves, their colleagues, or the interests of the organization can be factored into an employer's comprehensive insider threat analysis to determine whether that employee can continue to hold a position of trust in the organization.



DARK WEB

Activity on the Dark Web – online forums and exchanges related to guns, drugs, illicit pornography, hacking, and fraudulent financial activities – is often highly suspect. Although many legal activities take place in private areas of the Internet, Dark Web usage suggests that an individual would like to remain anonymous and may be engaged in or planning illegal activity. However, since Dark Web actors typically hide or limit access to their online forums through software that anonymizes users and encrypts communications, it is not entirely clear whether the information on such forums can be considered to be “publicly available”.

CONSIDERATIONS & RECOMMENDATIONS


Both public and private sector organizations must weigh the benefit of using PAEI for security and insider threat evaluations and come to a decision that fits their legal interpretations and corporate cultures. Below are some recommendations that all organizations should consider.

FEDERAL GOVERNMENT

A government decision regarding the use of PAEI for personnel security and insider threat purposes will set the standard for the use of such information by organizations in both the public and private sectors. Efforts to institute a continuous evaluation program for the government's trusted workforce – a critical element of initiatives to reform the security clearance process – have been hampered by agencies' inability to decide what PAEI sources are relevant to security determinations and whether and how to collect and assess employees' social media activities.

The Director of National Intelligence (DNI), as the government's Security Executive Agent, must work with the Defense Department, which is assuming government-wide investigation and adjudication responsibilities, to take several key steps:

1. *Decide, based on credible research, what sources of publicly available information are relevant to security determinations.* The Performance Accountability Council (PAC) – an interagency body chaired by the Office of Management and Budget (OMB) – has commissioned rigorous studies of some data sources, but it has not made a recommendation on what data should be consulted and how it should be weighed.
2. *Develop a single legal interpretation of what PAEI – including social media data – may be collected and analyzed for personnel security purposes.* Attorneys from the Defense Department and Intelligence Community agencies must, in conjunction with the Department of Justice, establish a common understanding of how these data can be used under the law. Otherwise, a security clearance granted by an agency that fails to consider social media could be rejected by an agency that requires evaluation of social media. A common legal interpretation is needed to set and implement common security standards.
3. *Develop policies for how PAEI – including social media data – may be used for security-related personnel determinations.* Clear government-wide policies, disseminated by the Security Executive Agent, are needed to ensure that PAEI, including social media posts, are collected, analyzed, and applied consistently across agencies.



Attorneys from the Defense Department and Intelligence Community agencies must, in conjunction with the Department of Justice, develop a single legal interpretation of what PAEI – including social media data – may be collected and analyzed for personnel security purposes.

PRIVATE ORGANIZATIONS

Private companies and other non-government entities must apply their own standards to determine if the organization is comfortable using PAEI for insider threat purposes. This decision-making is individualistic, often based upon an organizational culture and a cost-benefit analysis comparing the value of expected insider threat deterrence and detection versus the impact on employee morale and attrition. To minimize potentially negative workforce perceptions, some organizations may wish to make use of PAEI that is somewhat invisible to employees – such as commercially available databases containing information on personal finances, credit, law enforcement encounters, and the like – rather than information that employees feel more personally vested in, like social media content.

RECOMMENDATIONS

If an organization has decided to make use of PAEI for personnel security and insider threat purposes, the following practices can help it do so effectively.

1. Ensure leadership support

Leadership must endorse and promote the use of PAEI as a valid security tool that can be used in a manner consistent with the organization's mission, culture, and values. Without such leadership support, PAEI usage may cause resentment and pushback from the workforce.

2. Define and communicate internal policies

Organizations must codify in writing the rules that will govern the acquisition and use of data, and it should communicate these rules and their application to the workforce.

Organizations should develop written policies regarding the use of PAEI for new-hire vetting, insider threat evaluation, continuous evaluation, and other approved purposes. An organization may wish its policies to specify that the ways in which PAEI can be collected or consulted differ depending on the position of trust that an individual occupies; someone with access to sensitive information or networks may receive a higher level of scrutiny than someone holding a more routine position.

PAEI policies should also consider the extent to which employees take proactive measures to keep their data private. For example, if an employee's Facebook profile has no privacy settings and is open to any member of the platform, his/her Facebook posts can reasonably be considered "public". Similarly, if an employee has "friended" co-workers on Facebook who can see posts of worrisome behavior, an organization may consider it reasonable to evaluate conduct that such "friends" report to human resources officials or insider threat program managers no matter what privacy settings the employee has used. Such considerations should be evaluated by an organization's attorneys and addressed by its PAEI policy.

Organizations should incorporate consent language into hiring documents so that prospective employees are fully aware of, and consent to, PAEI-based monitoring before they begin onboarding. The government does this with the SF-86 form, which is completed by all job applicants seeking a security clearance – applicants for public trust positions complete an SF-85 – but other organizations may need to adjust their hiring documents.

To develop and maintain support for the policies, organizations should disseminate them to all employees and explain how they will protect the organization, its people, and its facilities. Leaders and managers should explain what information will be gathered – as well as what information will not be collected – and how it will be used for different purposes.

To promote trust in the PAEI policy and the organization's insider threat program more broadly, the policy should grant employees the ability to redress information used to make personnel decisions. Specifically, the individual must have access to the "raw" data collected from publicly available (and other) sources in order to challenge, correct, or dispute it.

An organization's policies should build support for an insider threat program among the workforce and help set clear processes for collecting, analyzing, and handling personal data. The absence of clear policies – or the failure to communicate them effectively – may lead employees to view the use of PAEI as counter to the organization's cultural norms and to view the organization with distrust.

3. Determine legal constraints

All insider threat programs must comply with existing privacy laws and regulations. Generally, the applicant or employee must be advised in writing on the use of PAEI for decisions about their employment, be offered a description of the nature and scope of the investigation and provide written permission. FCRA data requires employee release forms prior to PAEI collection and disclosure, but non-FCRA data does not. Identifying and resolving entities of interest without inadvertent collection on non-witting US persons is often done by hand to ensure compliance.

As a rule, social media checks on current and prospective employees can be legally conducted if the organization complies with the Fair Credit Reporting Act (FCRA), Equal Employment Opportunity Commission (EEOC), Security Executive Agent Directive (SEAD) 5 and other relevant state and federal laws.

4. Identify relevant information sources

Only activities that indicate an employee poses a potential risk to him/herself, co-workers, facilities, or sensitive information merit collection, analysis, and follow-up. Program managers should develop criteria that identify the kinds of data that are relevant to workplace security, the data sources that meet these standards, and the types of potentially derogatory insights that merit further investigation. On a regular basis, the PAC should report its research findings on what information is valuable in this regard so government agencies, cleared contractors, and other commercial organizations can use data-driven assessments to guide their use of PAEI.

5. Establish policies for the use of PAEI

Past behavior is not always an indicator of similar future behavior. Old expressions of support for an anti-democratic organization may not reflect a person's current beliefs or activities; previous self-destructive habits, such as excessive drinking or gambling, may no longer be an issue. Information on past actions must be evaluated in the context of an employee's current personal and professional behavior.

Rather than consider derogatory information identified through PAEI as a demonstration that someone is untrustworthy, insider threat program managers should treat such red flags as indicators that an in-depth evaluation may be needed. PAEI should not be used in isolation to make personnel decisions; it must be placed in the context of an individual's life. Data that an employee has taken out a second mortgage could indicate financial problems, or it could indicate that he/she is undertaking an expensive renovation to accommodate the needs of an elderly parent. Except in case of a potential imminent threat, PAEI should operate as a "tripwire" that identifies the need for additional research and analysis regarding an individual's broader behavior and life circumstances.

6. Assess timeliness, credibility and accuracy of PAEI

Some data is more current, and thus more relevant to a risk assessment, than others. Indications of long-ago financial difficulties, for example, may not accurately reflect one's current financial health, whereas a succession of loans in the previous 12 months is more likely to indicate that an employee has very recently faced cash flow problems. Some information is more conclusive than others; a record of an arrest indicates only that an employee may have engaged in criminal activity, while a conviction demonstrates proven criminal misconduct.

An organization must also have a way of assessing the credibility and accuracy of the data it consults. If it relies on a data aggregator of dubious credibility, it is more likely to receive false indicators of malicious activity and miss critical signs of risky behavior. In both cases, an organization will potentially allocate insider threat resources inefficiently, fail to mitigate risk, and alienate its workforce.

7. Determine how to efficiently process PAEI data

In both financial-related analytics and public records analytics, organizations are quickly overwhelmed when they seek to analyze flows of raw data. This is especially true of large government organizations, where data sets could represent millions of citizens. Organizations must adopt software tools that effectively ingest data determined to be relevant, ensure it conforms to organizational policies, compare it (or add it) to information gathered from internal sources, and package it for evaluation by a skilled insider threat analyst.

Many vendors offer scoring systems and analytics to qualify leads that generate actionable hits. These include standard adjudicative guidelines, standard deviations, customized business rules, financial models, or other proprietary formulas. The generated results can be used as input for an internal company analytics tool. A "trigger solution" is a methodology in which large data providers offer first-line analytics and provide only actionable information in a manageable format. This solution relieves the organization of the first-level analytics burden which allows the organization to then focus its resources on the much smaller high-risk segment of their population.

8. Ensure validity of data

Organizations should institute data validation processes to ensure that outside data is reliable and attributed to the correct employee. People with common names are often accused of, for example, owing a delinquent loan held by someone with the same or similar name. Because an unwarranted insider threat investigation could cause an individual significant professional harm, employers using outside data have a responsibility to validate the information and to prevent such errors.

9. Adapt to changes in data availability and evolving social mores

As technology evolves, it will make available additional sources of information on employee behaviors. The public's expectations of privacy – and laws governing privacy – will also change, in part to reflect new ways in which personal data is used. If a new source of information meets established criteria for relevance and usefulness in insider threat analysis, an organization should consider whether and how to incorporate it into its evaluation protocol. If, however, its relevance and value are negligible, insider threat program managers should resist making use of the data just because it becomes obtainable.

Organizations must continue to evaluate analytic tools, methodologies, and standards to ensure that analysis of raw data yields accurate and actionable assessments that reflect evolving standards and social mores. For example, reflecting the evolution in attitudes toward marijuana, an employer in a state that has legalized recreational use of marijuana may wish to stop considering social media posts showing personal use of the substance as a "red flag" indicating risky behavior.

CONCLUSIONS

As the U.S. Government reforms its security clearance process and implements a continuous evaluation program for members of its trusted workforce, it must develop government-wide legal interpretations and policy directives that tell agencies whether and how they can use PAEI – particularly employees' social media accounts and commercially available databases – to make informed risk assessments.

For the government, PAEI could enable clearance investigators to collect information more quickly and efficiently. The time saved would help eliminate the processing backlog, facilitate the hiring of cleared workers, facilitate the movement of cleared workers to where they can be employed most effectively, and reduce labor costs that are artificially inflated by the shortage of cleared workers. Government attempts to reform and improve the security clearance process must consider the dynamic growth in both data availability and data analysis technologies. Given this dynamism, the Security Executive Agent should regularly reassess whether to modify the PAEI sources used for continuous evaluation and to make clearance determinations.

The government's Security Executive Agent and the Department of Defense, which is assuming responsibility for conducting most clearance investigations and adjudications, should fund robust technology research and development and commission studies of how PAEI and other data can be used most effectively for employee screening and continuous monitoring. Toward this end, the government must partner closely with private sector firms that compile and analyze PAEI data and develop related analytic tools.

For both public and private sector organizations, PAEI can greatly improve the ability to identify malicious insiders before they cause damage to their information assets, people, or facilities. Private companies and other non-government entities must apply their own standards, based upon an organizational culture and a cost-benefit analysis comparing the value of expected insider threat deterrence and detection versus the impact on employee morale and attrition; Security Executive Agent guidelines on PAEI can serve as a baseline from which companies can develop their own PAEI standards.

Background investigations and insider threat assessments seem intrusive to many people, and the use of PAEI can make such processes seem even more invasive. However, given the harm caused by espionage, the theft of intellectual property, and workplace violence, it is worth the investment of time and resources to determine how PAEI can be used to protect national security, valuable assets, and human life.

ACKNOWLEDGEMENTS

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

INSA MEMBERS

Val Letellier, *CACI*
Greg Cullison, *Big Sky Associates*
Catherine Albright, *Thomson Reuters*
Bryan Denson, *TransUnion*
Randy Fort, *Raytheon*
Mike Hudson, *ClearForce*
Deborah Johnson, *Jacobs*
Steve Lewis, *Omniplex*
David Luckey, *RAND Corporation*
Matt Miller, *Goldman Sachs*
Sandy Maclsaac, *Deloitte*
Chair, Insider Threat Subcommittee
Vince Corsi, *IBM*
Vice Chair, Insider Threat Subcommittee

INSA STAFF

Chuck Alsup, *President*
Larry Hanauer, *Vice President for Policy*
Peggy O'Connor, *Director, Communications and Policy*
Ehrl Alba, *Digital Marketing Manager*
Bill Harley, *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