



**INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE**



OCTOBER 2020

Mitigating Advanced Persistent Insider Threats Fueled by Major Data Breaches

Presented by

INSA'S INSIDER THREAT SUBCOMMITTEE

INTRODUCTION

Large-scale thefts of personal data threaten American government agencies and private companies that hold sensitive information of value to hostile nations. Data breaches at the U.S. Office of Personnel Management (OPM), Anthem Health, Equifax, Yahoo, Marriott, United Airlines and multiple online dating sites – among many others – help America’s adversaries target, exploit, and even recruit sources inside government agencies, businesses, and universities.

These breaches played an integral role in shaping the new national strategy to prevent counter-espionage threats against the United States, which was recently announced by the National Counterintelligence and Security Center (NCSC), part of the Office of the Director of National Intelligence (ODNI). The strategy states that: “Threats to the United States posed by foreign intelligence entities are becoming more complex, diverse, and harmful to U.S. interests,” and “threat actors have an increasingly sophisticated set of intelligence capabilities at their disposal and are employing them in new ways to target the United States.” China is the most active and threatening adversary using refined targeting to steal American intelligence and technology. However, Russian and Iranian intelligence organizations are also known to use false social media personas to target Americans of interest through both virtual and personal means.

These newfound intelligence capabilities include advanced data analytics and technology that are strategically designed to exploit the systems and infrastructure of various U.S. entities. This combination of advanced capabilities and the collection of sensitive personal data obtained through major breaches and various social media platforms creates a ‘perfect storm’ for taking advantage of insiders’ vulnerabilities in government, industry, and academia. Given the wide range of data on American citizens that has been stolen within the last five years – encompassing information on individuals’ security clearances, travel, health, and finances, as well as highly personal information revealed on dating sites – our adversaries have a far more comprehensive picture of those trusted by our government and its outside partners than ever before.

The information obtained from these large-scale breaches can now be aggregated and analyzed with more current personal data to identify Americans with access to national security information, technology research, and valuable intellectual property (IP). This same information can then be used to identify specific behavioral, financial, and medical variables that will help determine an individual's vulnerability to a clandestine or a remote technical approach.

This type of advanced persistent insider threat (APT) is extremely dangerous. State-backed attackers tend to be professional and well-resourced, relentlessly focused, and able to deflect traditional countermeasures. Regrettably, most U.S. institutions are unprepared for this threat; they lack awareness of how adversaries can use stolen information to target their employees and are ill-equipped with countermeasures to detect and mitigate attacks.

That said, resiliency is attainable. By developing the right approach, organizations can harden their workforces to thwart adversarial attempts at major breaches. A strategic posture including proactive risk-based decision making, a connected and cared for workforce, and a "whole person" / "whole threat" approach will help create a positive and effective security culture. Policies that advance effective governance, awareness training, reporting mechanisms, continuous evaluation, and employee accountability will reinforce such a strategy. Information security measures, such as encrypting data at rest, will help prevent an adversary from exploiting stolen records. Collectively, these measures will help organizations mitigate advanced persistent insider threats.

WHY STEAL THIS DATA?

If you are a foreign adversary and your goal is to efficiently identify, assess and engage Americans involved in national security, intelligence and advanced technology research, you would aggressively seek out the legal, health, financial, travel and personal relationship details of those considered for government security clearances. By applying modern data analytics – such as artificial intelligence (AI) and machine learning (ML) tools – to massive data sets, targeted individuals' interests and patterns of life can be discerned, providing adversaries with critical details around which a viable personal or virtual recruitment approach can be constructed. Experts assess that Chinese military and/or intelligence services were responsible for the data breaches at Marriott¹ and Equifax.² Chinese hackers are believed to be behind the breaches of OPM, Anthem,³ United Airlines, and Yahoo; although conclusive links to government agencies have not been publicly revealed, it is reasonable to assume that Chinese security services – even if they did not direct these breaches – have managed to gain access to valuable data stored on servers in China.



Given the wide range of data on American citizens that has been stolen within the last five years – encompassing information on individuals' security clearances, travel, health, and finances, as well as highly personal information revealed on dating sites – our adversaries have a far more comprehensive picture of those trusted by our government and its outside partners than ever before.

U.S. adversaries are already in a position to develop such highly tailored targeting approaches. Several large-scale data breaches revealed personal data on millions of Americans with access to government secrets and valuable corporate intellectual property. Among the most notable such breaches are:

- The OPM breach (itself facilitated through the theft of an insider’s credentials), which was revealed in June 2015, exposed the records of approximately 22 million civilian employees, contractors, and military personnel who hold security clearances. This included sensitive Personally Identifiable Information (PII), along with highly personal information that must be disclosed to secure a clearance, such as records of individuals’ debts, arrests, drug and alcohol use, and foreign associations – all information that can be used to blackmail someone, exploit their vulnerabilities, or develop a targeted approach to them.⁴
- The Yahoo breach, which was disclosed in 2016, provided access to phone numbers, password challenge questions/answers, and alternate email addresses of many of the company’s three billion users, all of which can be used to gain access to an individual’s other online accounts. The breach also exposed users’ email communications, which gave adversaries insights into their personal and professional activities, contacts, relationships, and stances on social and political issues.⁵
- The 2015 Anthem breach exposed the health insurance details of nearly 80 million Americans. Such insights could be used to exploit someone’s emotional stresses, family tensions, and – given the high cost of many medical treatments – financial vulnerabilities.⁶
- Marriott’s Starwood breach, which took place in 2014 but was not revealed until late 2018, exposed nearly 400 million individual records, which provide insights into guests’ travel patterns, partners, and preferences. It is likely not a coincidence that attackers targeted Marriott, which is the largest hotel provider for U.S. government and military personnel.⁷ The stolen data also included up to five million passport numbers containing personal data like individuals’ dates and places of birth.



- The 2015 breach of Ashley Madison – a site catering to married people seeking affairs – exposed potential blackmail material on 40 million members. Hackers posted user names, addresses, and phone numbers for 32 million Ashley Madison users on the Dark Web, where they could be acquired by hostile intelligence services. Approximately 15,000 of the leaked e-mails were .gov or .mil addresses.⁸ A breach of Adult FriendFinder, a similar dating service, exposed data on 412 million users a year later.⁹
- Finally, the Equifax breach exposed the personal financial records of nearly 150 million Americans, including earning and spending histories, personal debt loads, foreclosures, and late payments.¹⁰

This begs the question – beyond updates to the above-noted personal data, what more could our adversaries want? A recent Pentagon decision to ask military personnel to stop using at-home DNA analysis kits like ‘23andMe’ and ‘Ancestry’ may suggest that DNA is the next big data pool to be targeted. These unique and unchangeable ‘digital fingerprints’ will likely play a significant role in future biometric technologies and methodologies.¹¹

WEAPONIZING THE STOLEN DATA

According to reports from the FBI and the Cybersecurity and Infrastructure Security Agency (CISA), malicious actors already “compile dossiers on the employees at the specific [targeted] companies using mass scraping of public profiles on social media platforms, recruiter and marketing tools, publicly available background check services, and open-source research.” Such easily available information provides insights into the nature of a person’s work, expertise, and information access, which helps identify targets of interest. When combined with highly personal data stolen from a healthcare, travel, or government personnel office an attacker can develop a comprehensive targeting package with insights into an individual’s motivations, vulnerabilities, character, and activities. This precise targeting improves the likelihood that a malicious actor will be able to successfully approach a target with access to desired information and eventually lead to the clandestine transfer of sensitive national security information or intellectual property.

Consider how an adversary might combine open source and stolen data to identify and target a U.S. citizen with access to sensitive information.

- To spot a target of potential interest, targeters search the Internet and find a LinkedIn profile, reports from college alumni magazines, and a published article that together suggest that Person X works in a government office in which he would likely have access to classified information on a program of interest. Using data from the person’s stolen SF-86 security clearance application form, targeters verify the person’s expertise from a detailed listing of previous jobs, verify that he has held clearances in the past, and surmise that his clearance remains active. The person’s value as a potential source of useful information is confirmed (If the U.S. person is determined not to have access to information of interest, attackers can review LinkedIn contacts or read stolen personal emails to identify others who might).
- To assess the target’s vulnerabilities to persuasion or coercion, targeters also mix a range of data. For example, the attacker might see that the person has self-reported financial difficulties on his SF-86. Drawing on the person’s credit report in stolen Equifax data, targeters see that the person continues to struggle with debt. They also see that his salary has increased very little in recent years, suggesting that he has not been promoted in a while. A review of stolen healthcare data reveals that a dependent family member has a long-term medical condition requiring expensive treatments, even with insurance. Now the attacker knows that the person has financial difficulties, a highly stressful family situation with significant financial implications, and potential resentment over not being promoted or paid more. Targeters can surmise that the person would have a potential interest in outside financial remuneration. If the person’s name and personal preferences appear in stolen online dating data, the adversary may be positioned to blackmail them into cooperating.
- To determine how to approach the target, the adversary reviews stolen travel data from Marriott. They identify a pattern of regular travel to three foreign cities. They provide the target’s passport number, hotel loyalty number, and other data to contacts at the hotel company who can alert them to the target’s upcoming trips. Now the adversary knows where they can meet the target outside the United States to make a pitch. Using insights into the person’s interests, contacts, and education and work history from stolen email messages, SF-86 forms, and publicly available social media posts, an adversary can make an innocuous and friendly introduction – even purporting to have several experiences or contacts in common.

A pitch does not need to explicitly propose espionage for a hostile foreign state. The pretext used in any social engineering effort may include a cover story, or 'false flag' element, to hide the attacker's true affiliation and portray an identity more acceptable to the employee. Offers of paid part-time consulting, research, or conference participation are common and fruitful tactics used by attackers to begin administering control and financial dependence – and to elicit information that the person really shouldn't be providing. Individuals may not even know they are being targeted and revealing sensitive information until it's too late – by which time the adversary has significant leverage over the person.

An approach can also be purely virtual. If the targeted information can be stolen entirely through virtual means, the attacker's targeting package could be used to 'spear phish' the target with a highly tailored and credible electronic message based on information gleaned from both open-source and stolen personal data; in August 2020, the FBI even warned that criminals armed with personal data have begun to use voice calls to elicit user credentials and other sensitive information, a process called "vishing," which potentially makes the elicitation more personal and thus less threatening. The subsequent deployment of malicious software can provide the attacker access to the user's device, from which they can steal credentials and eventually capture the sought-after information.

CRAFTING AN EFFECTIVE STRATEGY

How is an organization to respond when adversaries have detailed personal information about many of its employees? While an advanced persistent insider threat mitigation strategy must be tailored to an organization's risk profile, culture, and resources, effective insider threat programs share several traits that leaders in both government agencies and private companies should work to implement.

PROACTIVITY. Organizations can 'get ahead of the game' by intervening early and engaging positively with distressed employees before adversaries can exploit deteriorating situations.



A cohesive workforce enhances organizational resiliency to insider attacks. Employees who know each other well are better able to identify anomalous behavior in a colleague and are thus positioned to intervene with their co-worker or report concerns to management.

RISK-BASED DECISION-MAKING. Too often, leaders treat insider threat as something that simply happens, is driven by unpredictable and unexplainable human nature, or is impossible to preempt or prepare for. A far more effective approach to all insider risk – and specifically the advanced persistent threat – is to treat it as a likely, if uncommon, occurrence driven by recognizable risk factors that has predictable ramifications which can be lessened through preemptive action. Organizing risk information by probability and outcome, into a broad and orderly structure, empowers decision-makers to make informed and improved choices.

A CONNECTED WORKFORCE. A cohesive workforce enhances organizational resiliency to insider attacks. Employees who know each other well are better able to identify anomalous behavior in a colleague and are thus positioned to intervene with their co-worker or report concerns to management.

“

...greater compliance with security measures. By providing counseling and other assistance to employees showing warning signs of financial, legal or emotional stress – such as through an Employee Assistance Program (EAP) – an organization can transform workers from potential liabilities into employees who appreciate the organization’s concern for their well-being.

A ‘WHOLE PERSON’ AND ‘WHOLE THREAT’

APPROACH. Holistic methodologies are the key to effective insider threat detection and prevention. A ‘whole person’ approach is contextual and psychosocial, using access, personality, environment, and precipitating events to identify insider threats. It considers a person’s inherent dispositions and the stressors that can push a person towards insider attacks. A ‘whole threat’ approach addresses the common root causes of attacks. These methods assess trusted insiders and identify the precipitating events that can turn certain personalities toward malicious action. For example, the common personality traits of a malicious insider who has stolen sensitive information include entitlement, narcissism, antisocial behavior, and a desire for control. Usual precipitating events include a negative personal financial event, failed promotion, poor performance review, unfulfilled career aspirations, resignation, or termination. This profile is different from an insider who attacks through fraud, sabotage, or physical violence. Awareness and understanding of specific advanced persistent threat ‘tripwires’ can strengthen insider threat mitigation efforts.

A POSITIVE SECURITY CULTURE. Building trust with the workforce is paramount. Communicating honestly and often about efforts to protect employees and their jobs will help build a grassroots security culture that results in greater compliance with security measures. By providing counseling and other assistance to employees showing warning signs of financial, legal or emotional stress – such as through an Employee Assistance Program (EAP) – an organization can transform workers from potential liabilities into employees who appreciate the organization’s concern for their well-being.

TRAINING. Employees – but particularly those whose information is believed to have been compromised – should receive training on how to recognize signs they are being targeted.



SUCCESSFUL IMPLEMENTATION OF THE STRATEGY

While a range of best practices can serve to strengthen insider threat programs, the following are most relevant to mitigating advanced persistent insider threats:

ENGAGE EMPLOYEES. It bears repeating that there is no insider risk countermeasure as valuable as personal knowledge of an organization's trusted employees. This is particularly true in the COVID era, when employee engagement is critical if the organization is to assess morale, unity, and health—both physical and mental.

DRAFT EFFECTIVE GOVERNANCE POLICIES.

Security policies and procedures are the defensive building blocks upon which all security measures rest. Employees' access to critical data or materials should be limited based on their roles, the nature of information, and need-to-know principles. Organizations may need to consider and draft effective policies for authentication, secure communication, encryption, personal device usage, data and device storage, and employee monitoring. It should also detail how technical controls for insider threat monitoring and a multi-layered defense will be used to improve early detection of anomalous behavior and large data exposures. Finally, policies should ensure that public data is properly collected and used, and that technical controls for insider threat monitoring are regularly tested to ensure they are configured correctly.

BE OPEN AND TRANSPARENT. Communication helps secure employee buy-in and support and serves as a warning to employees who find themselves targeted. Managers can clearly convey what insider threat programs do and why, and explain that they are designed to protect both employees and the organization. By explaining that the program is meant to provide early identification of employees who may need assistance, the program will likely be viewed as positive rather than punitive.



Security policies and procedures are the defensive building blocks upon which all security measures rest.

IDENTIFY ALL ACCESS POINTS. Generally, this list is significantly longer than most risk managers realize, and even more so with those working on a client site or from home. In remote work situations, critical data is often handled in an uncontrolled environment where an organization has limited ability to monitor security policy adherence or to ensure that data remains only with those designated to receive it. Technicians or vendors with access to offices or to networks housing critical data are often overlooked. Attackers likely will determine all available paths to the specific information they seek and will exploit the one that is least protected – such as someone whose access to certain networks or material is not widely known. In 2013, for example, hackers stole 40 million credit card numbers from Target by using network credentials stolen from a heating and air conditioning subcontractor.

LEVERAGE PEOPLE AND TECHNOLOGY. Insider threat early warning is truly a ‘team sport’ requiring both human and technical sensors. Human resources (HR) can highlight performance and behavioral issues, information technology (IT) can highlight network anomalies, and security can highlight policy violations. Line managers and fellow employees are particularly valuable sensors; they subconsciously create behavior baselines for everyone they know, recognize deviations from those baselines, and evaluate what they see within context. Finally, public data is a highly valuable early warning tool that should be considered under certain circumstances.

DEVELOP THREAT AWARENESS AND ACCOUNTABILITY. Employees should be taught to recognize warning signs of distressed employees, along with the ways to safely and easily report anomalous behavior. Employees should be taught to recognize, resist, and report attempts to compromise or recruit them. Organizations may want to make it mandatory for employees to report security violations, as the existence of a rule can make it easier to justify “turning in” a colleague.



Positive intervention is what is needed (e.g., deal with employee conflict, manager issue). EAP can ensure support in place for an employee whose personal issues are flowing into [the] workplace. For the most part, employees want to do the right thing. They just often do it in a very wrong manner.

TEST EARLY WARNING CAPABILITY. Objective testing of organizational resiliency is critical to understanding an organization’s weaknesses and resource requirements.

1. The first step is an internal assessment of policies, procedures, and actual behavior.
 - Assess the adequacy of policies and the workforce’s adherence to those policies.
 - Look at the workforce’s understanding of insider threat indicators and how to report and respond to them.
 - Measure the cohesion between managers and workers.
 - After looking within, analyze outsiders who require a certain level of trust—such as vendors, subcontractors, and others with privileged access to the organization or its assets.
2. Second is a tabletop exercise to simulate the actions of an advanced persistent insider, determine how anomalous activity can be identified and by whom, and assess the organization’s response. New policies and procedures should address weaknesses identified during the exercise.
3. The third is outside red-teaming. It is difficult for organizations to stop attacks they can’t conceive of by threat actors whose interests and capabilities they don’t understand. Outside perspectives can help organizations understand what they have that is of value to others, predict how an attacker would act, and identify a network’s critical vulnerabilities.

CONTINUOUSLY MONITOR. Humans evolve in response to factors internal and external to the organization. Internally, an employee may be assigned a role seen as a demotion; externally, he could become financially vulnerable within a few months of taking on a debt or having a spouse lose a job. Continuous evaluation can help identify a deteriorating situation in near-real-time, thus enabling the organization to mitigate it before it becomes critical. Continuous evaluation can take several forms:

- **Human observation:** With a positive security culture and informed workforce, line managers and colleagues serve as “human sensors” that can identify anomalous behavior.
- **Network data:** A wide array of data analytic methods, tools, and techniques exist to improve the detection and mitigation of insider threats. User behavior analytics (“UBA”) help organizations identify intrusions and/or anomalous activity. User and entity behavior analytics (“UEBA”) tools analyze log and event data from applications, endpoint controls, and network defenses. Big data techniques help determine patterns of behavior, and employee monitoring software captures all network activity. Finally, advanced enterprise monitoring solutions can look for particular keywords or sentiments.
- **Public data:** Financial, law enforcement, and court records can be used to flag concerning behavior in real-time. Because incorporating public data into insider threat programs has significant privacy and civil liberties implications – no organization wants its employees to think Big Brother is monitoring their personal lives – organizations must weigh the benefits and drawbacks of using such data before coming to a decision that aligns with their corporate culture. ■■■■■

CONCLUSION

The advanced persistent insider threat is far from focused on U.S. Government agencies and technology innovation firms. In February 2020, FBI Director Christopher Wray told the U.S. Department of Justice’s China Initiative Conference that China is “not just targeting defense sector companies. The Chinese have targeted companies producing everything from proprietary rice and corn seeds to software for wind turbines to high-end medical devices. And they’re not just targeting innovation and R&D. They’re going after cost and pricing information, internal strategy documents, bulk Personally Identifiable Information (PII) – anything that can give them a competitive advantage.” Private industries as varied as ocean engineering, artificial intelligence, and vaccination research are witnessing a spike in unwanted foreign attention.



Implementing proactive measures, taking the time to get to know employees, employing risk-based decision-making, and embracing a whole person/ whole threat approach, will help organizations create holistic resiliency greater than the sum of its component parts.

Now is a critical time for risk managers to fortify their organizations. Advances in machine learning, artificial intelligence, and 5G networks are making data collection more ubiquitous and data aggregation more capable. Finally, the COVID-19 pandemic is making current and former employees with access to sensitive information more financially, psychologically, and technologically vulnerable. Implementing proactive measures, taking the time to get to know employees, employing risk-based decision-making, and embracing a whole person/ whole threat approach, will help organizations create holistic resiliency greater than the sum of its component parts. By hardening their organizations, leaders are helping to protect sensitive defense and intelligence data, secure technological advancements, enhance government and industry effectiveness, and minimize the negative impact of future breaches. ■■■■■

REFERENCES

- ¹ David Sanger, Nicole Perloth, Glenn Thrush, and Alan Rappeport, "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *New York Times*, December 11, 2018. At <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>.
- ² Devlin Barrett and Matt Zapotosky, "U.S. Charges Four Chinese Military Members in Connection with 2017 Equifax Hack," *Washington Post*, February 11, 2020. At https://www.washingtonpost.com/national-security/justice-dept-charges-four-members-of-chinese-military-in-connection-with-2017-hack-at-equifax/2020/02/10/07a1f7be-4c13-11ea-bf44-f5043eb3918a_story.html.
- ³ Corey Bennett, "OPM Hackers Suspected in United Airlines Breach," *The Hill*, July 29, 2015. At <https://thehill.com/policy/cybersecurity/249601-opm-hackers-may-have-hit-united-airlines-as-well>.
- ⁴ Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, July 9, 2015. At <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>.
- ⁵ Nicole Perloth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," *New York Times*, October 3, 2017. At <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>.
- ⁶ Department of Justice, "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People," press release, May 9, 2019. At <https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including>.
- ⁷ Sanger, Perloth, et. al.
- ⁸ Kim Zetter, "Hackers Finally Post Stolen Ashley Madison Data," *Wired*, August 8, 2015. At <https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>.
- ⁹ Andrea Peterson, "Adult FriendFinder Hit with One of the Biggest Data Breaches Ever, Report Says," *Washington Post*, November 14, 2016. At <https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says/>.
- ¹⁰ Nathan Bomey, "How Chinese Military Hackers Allegedly Pulled Off the Equifax Data Breach, Stealing Data From 145 Million Americans," *USA Today*, February 10, 2020. At <https://www.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/>.
- ¹¹ Ellen Matloff, "Why the Pentagon Is Warning US Military Not to Use Recreational Genetic Test Kits," *Forbes*, December 27, 2019. At <https://www.forbes.com/sites/ellenmatloff/2019/12/27/why-the-pentagon-is-warning-us-military-not-to-use-recreational-genetic-test-kits/#40941b5b3d56>.
- ¹² Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA), "Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign," *Joint Cybersecurity Advisory*, Product ID: A20-233A, August 20, 2020. At <https://krebsonsecurity.com/wp-content/uploads/2020/08/fbi-cisa-vishing.pdf>.
- ¹³ Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA), August 20, 2020.
- ¹⁴ See, for example, Catherine Stupp, "As Remote Work Continues, Companies Fret Over How to Monitor Employees' Data Handling," *Wall Street Journal*, August 21 2020. At <https://www.wsj.com/articles/as-remote-work-continues-companies-fret-over-how-to-monitor-employees-data-handling-11598002202>.
- ¹⁵ Reuters, "Target Settles 2013 Hacked Customer Data Breach For \$18.5 Million," May 24, 2017. At <https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031>. See also "Target Hackers Broke in via HVAC Company," *Krebs on Security*, February 5, 2014. At <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>.
- ¹⁶ Christopher Wray, "Responding Effectively to the Chinese Economic Espionage Threat," Department of Justice China Initiative Conference, Center for Strategic and International Studies, Washington, D.C., February 6, 2020. At <https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat>.



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, *Perspecta*;
Insider Threat Subcommittee Vice Chair

Val Letellier, *Raytheon Technologies*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

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

Caroline Henry, *Marketing & Communications Assistant*

Rachel Greenspan, *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.