ASSESSING THE MIND OF THE MALICIOUS INSIDER:

USING A BEHAVIORAL MODEL AND DATA ANALYTICS TO IMPROVE CONTINUOUS EVALUATION

Prepared by

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

SECURITY POLICY REFORM COUNCIL

INSIDER THREAT SUBCOMMITTEE

April 2017

INSA

ACKNOWLEDGEMENTS

INSA appreciates the efforts of everyone who contributed to the research and production of this white paper:

MEMBERS OF THE SECURITY POLICY REFORM COUNCIL AND INSIDER THREAT SUBCOMMITTEE

Charlie Allen, *Chair*
The Chertoff Group

Katherine Hibbs Pherson, *Vice Chair*
Pherson Associates

Doug Thomas, *Insider Threat Subcommittee Chair*
Lockheed Martin

Vincent Corsi
IBM

Mark Gardiner
BAE Systems

Sandy MacIsaac
Deloitte

Daniel McGarvey
Alion Science and Technology

Renee Thompson
Deloitte

INSA LEADERSHIP

Letitia A. Long, *Chairman*

Chuck Alsup, *President*

INSA STAFF

Larry Hanauer, *Vice President for Policy*

Ryan Pretzer, *Policy and Public Relations Manager*

English Edwards, *Marketing and Communications Manager*

Katy Petyak, *Intern*

ADDITIONAL THANKS TO:

Joseph Lualhati
Global Skills Exchange

Charles S. Phalen
Director, National Background Investigations Bureau

Dr. Jerrold Post
U.S. Intelligence Community (former)

INSA SUPPORTS A HEALTHY PLANET

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

> The model in this paper assumes that an initially loyal employee does not suddenly transform into a malicious insider.

EXECUTIVE SUMMARY

Insider threat detection is one of the most difficult challenges facing industry and the Intelligence Community (IC) today. With roughly three million individuals cleared to access classified information[1] and a multitude of ways to compromise it, determining who may pose a significant threat at a particular point in time is a monumental task. The key to improving an organization's prospects for preventing a major malicious act is knowing what behaviors to look for and having effective monitoring tools in place.

This paper reviews and integrates several accepted psychological constructs into a behavioral model that can be adapted for practical use and suggests new tools to leverage this model to mitigate threats from insiders who may intentionally decide to harm their organization or our national security. It continues the exploration of security issues in two earlier INSA papers: "Leveraging Emerging Technologies in the Personnel Security Process,"[2] which offered ways to continuously evaluate and monitor those accessing sensitive information, and "A Preliminary Examination of Insider Threat Programs in the US Private Sector,"[3] which sought ways to assess and compare industry's initial implementation of Insider Threat programs.

The model of behaviors in this paper, derived from a body of research studies on malicious insiders, assumes that an initially loyal employee does not suddenly transform into a malicious insider. Certain personality traits may predispose an employee to acts of espionage, theft, violence, or destruction. These traits may be reinforced by environmental and organizational stressors. Less severe counterproductive work behaviors commonly occur before the decision to initiate a major damaging act. Clustering these behaviors into families may help define an "early warning system" and improve understanding of how individual characteristics and environmental factors may mitigate or intensify concerning behaviors.

Effective monitoring tools that can work in tandem with this model take advantage of technology to surpass standard screening for biographic factors (i.e. criminal record, financial history) or the monitoring of computer activity. In particular, advanced text analytics and psycholinguistic tools that track an employee's communications across social media and other platforms to detect life stressors and analyze sentiment can help detect potential issues early in the transformation process. Another critical element is improving the sharing of information within organizations among managers, human resources, information technology (IT), security, and legal advisers regarding minor counterproductive work behaviors that may indicate an employee is struggling and at heightened risk of committing a malicious act.

> Advanced text analytics and psycholinguistic tools can help detect potential issues early in the transformation process.

Introducing sophisticated new tools and effective monitoring immediately raises a host of questions that require further discussion to assess how best to incorporate them in Continuous Evaluation programs. These include how to balance privacy and security, assess the impact on workplace morale, determine the triggers for undertaking additional monitoring and action, and incorporate oversight and protections for civil liberties. We anticipate that organizations will reach very different outcomes depending on their institutional cultures. In the end, this is a critical risk management exercise for senior leaders in all organizations as the destructive power of malicious insiders grows and the tools to monitor and mitigate become more sophisticated and intrusive.

INSA's Security Policy Reform Council recommends a number of follow-up initiatives to further explore the key concepts outlined in this paper, focusing in particular on validating the use of behavioral models and automated tools to identify at-risk individuals and to design mitigation strategies that help employees change course – or that remove employees' access to sensitive data, systems, and facilities – before they commit malicious acts. Both government and industry have significant equities and interest in making progress to improve insider threat programs. INSA is committed to creating partnerships and forums to advance both research and dialogue on these complex issues.

UNDERSTANDING HOW TRUSTED INSIDERS BECOME MALICIOUS

Preventing loss of sensitive information – or, more recently, violence in the workplace – is now more than ever a top priority in the Intelligence Community. It has taken on an unprecedented urgency because of high profile losses of information, intelligence capabilities, and lives. We are painfully aware that our old ways of doing business are not up to protecting our workplaces given the ease with which large amounts of automated data can be compromised with a keystroke or the challenge of deterring violent loners in our globalized, fast-paced world. Reviewing what we know about malicious insiders can help us improve our ability to recognize and potentially divert them from destruction.

PSYCHOLOGICAL CHARACTERISTICS

Studies over the past several decades within and outside government have focused on psychological aspects of spies and traitors, including the work of former Central Intelligence Agency (CIA) psychiatrist Dr. Jerrold Post. In the late 1990s, Post and his colleagues Eric Shaw and Keven Ruby at Political Psychology Associates completed a two-year study for the Department of Defense (DOD) on Insider Threats to Critical Information Systems. Based on interviews, literature reviews, and case studies, the team identified a cluster of psychological characteristics shared by those deemed to be at increased risk for undertaking damaging insider acts and related them to two clusters of well-known personality disorders. (See Figure 1.)[4]

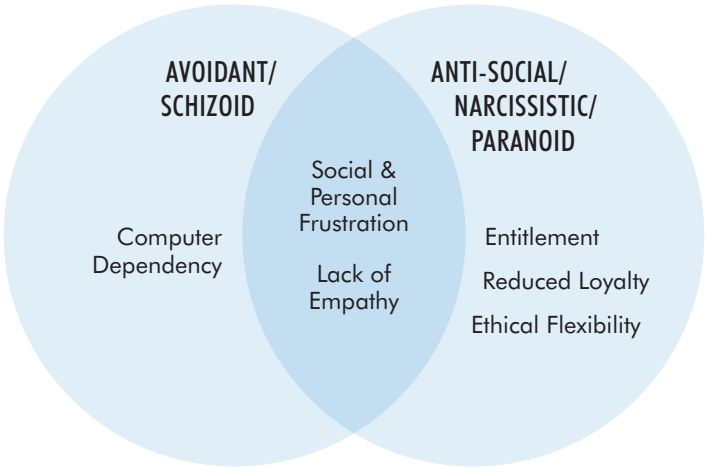

Figure 1: Vulnerable Information Technology Insider Characteristics and Personality Clusters

One of these, the narcissistic/anti-social personality type, is the type most prevalent in studies of those who commit espionage. It is associated with preoccupation with personal needs and reduced empathy for others, absent or deficient conscience, low self-esteem, and sensitivity to slight. These traits, however, relatively rarely lead an individual to commit malicious acts. Post, et al describe these individuals as being on a "critical pathway"; their movement from loyalty to destruction depends on how they relate to stressors in their personal and organizational lives and how the organization reacts – or fails to react – to signs of employee distress or disgruntlement.

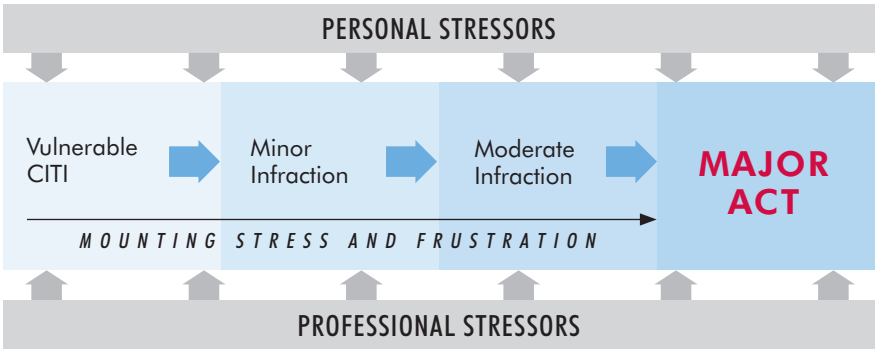

Figure 2: Pathway to Major Malicious Acts

In the second year of the study, Post, et al concluded[5] that the pathway to a major act is littered with minor and moderate infractions that grow in response to mounting stress and frustration. (See Figure 2.) Vulnerabilities associated with greater likelihood of espionage or sabotage include social and personal frustrations, ethical flexibility, reduced loyalty, sense of entitlement, lack of empathy, and anger at authority. The lack of recognition or response by the organization in many cases encouraged the employees' sense of entitlement and reduced their sense of accountability for their own actions. Effective management that deals with the minor lapses can create mitigating forces and perhaps rescue "vulnerable critical IT insiders (CITIs)" from becoming "dangerous CITIs" (see Figure 3),[6] who may eventually betray the organization.

LIFE STAGES

A similar conclusion was reached more recently by Dr. David Charney,[7] who characterized the insider's evolving critical pathway in terms of ten life stages. Based on interviews with three prosecuted "insider spies" (Robert Hanssen, Earl Pitts, and Brian Regan) and case studies of traitors from different countries, Charney likewise noted that acts of treason are often end points of cold, bitter, building resentment against a system they perceive to have insufficiently recognized and rewarded them. The perpetrators are not "born bad" or characterized by fixed, predictable personality traits.

This life cycle provides a useful framework within which to observe those on the critical pathway in terms of how they perceive and deal with their own success or failure. During the mid-life transition between 35 and 45 years of age, individuals tend to reevaluate their lives, their choices, and their goals. The symbiotic relationship between personal and professional lives is significant during this time, when divorces and career changes typically peak. A strong personal relationship can help individuals weather a period of job dissatisfaction. Similarly, a positive work environment and feelings of professional reward can carry them

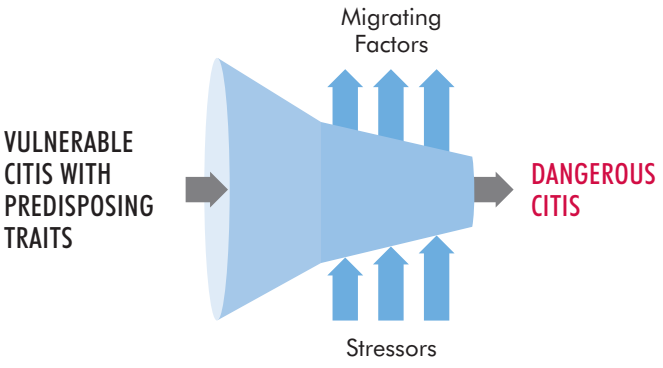

Figure 3: Critical Pathway with Stressors and Mitigating Factors

through a period of marital stress. Simultaneous marital and professional stress creates major psychological vulnerabilities. Post notes that nearly all of the major agents-in-place and defectors were impelled to act during this life period.[8]

COUNTERPRODUCTIVE WORK BEHAVIORS

The substantial body of research in counterproductive work behaviors (CWB) – employee behavior that goes against the legitimate interests of the workplace[9] – provides a third lens through which to understand how the insider's critical pathway can be observed in the real world. The stress that results from negative life events on the job and in personal lives can lead, if unmitigated, to problematic behaviors in the workplace.

Several typologies have been proposed to categorize these behaviors along multiple dimensions, including the type (deviance from accepted behavioral norms); the target (the organization vs. the people working within it); the severity of the behavior (minor vs. serious); and whether the behavior is directed against work processes or assets (production vs. property).[10] Based on the target of the behavior, CWBs are generally categorized as actions intended to harm the organization (organizational deviance, or CWB-O) or to harm fellow employees (interpersonal deviance, or CWB-I).

CWB research provides three insights that are key to detecting and mitigating employees at risk for committing damaging insider acts:

- *CWBs often co-occur.* An individual who engages in one type of CWB will be more likely to engage in several, underscoring the need to focus on patterns and families of behaviors as potential indicators of larger problems.
- *CWBs usually escalate.* Less severe incidents lead to more severe incidents, suggesting the need for managers to understand the pattern and be skilled in minimizing escalation.
- *CWBs seldom occur spontaneously.* Stress at home or at work adds to the potential for counterproductive workplace behaviors, particularly in individuals with vulnerable personality characteristics.[11] This means employers need to pay particular attention to changes in behaviors that might relate to employee dissatisfaction and devise strategies for action suited to the individual.

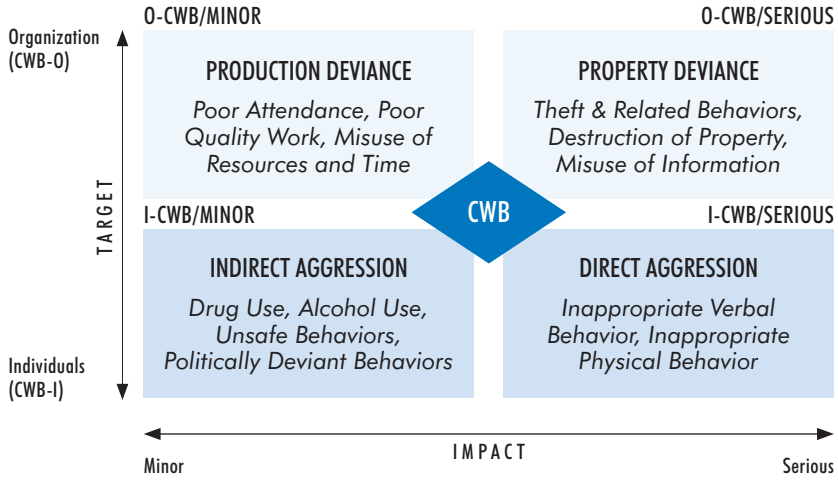

Figure 4: A Framework for Relating Counterproductive Work Behavior to Insider Threat

In relating this literature to the insider threat, Joseph Lualhati and Daniel McGarvey, in work on behalf of ASIS International's Defense & Intelligence Council,[12] proposed combining these aspects into a framework of workplace misbehavior (see Figure 4) that can be used by security and human resource professionals and managers to categorize employee behaviors that might indicate movement along the critical pathway toward a dangerous action. This approach aligns with the findings and recommendations of Post, et al.

Using existing CWB categories and the Diagnostic and Statistical Manual of Mental Disorders Vol. 5 (DSM-5)[13], Lualhati and McGarvey also offered an initial taxonomy of families of concerning behaviors relating to insider threat. This approach is based on work by DoD's Personnel Security Research Center (PERSEREC)[14, 15] demonstrating that selected personality disorders defined by the predecessor volume to the DSM-5 could be linked to the personnel security adjudicative criteria and quantified to provide additional data to adjudicators.[16]

To create the taxonomy, Lualhati and McGarvey listed families of negative insider behaviors under two well-known constructs – the Stressor-Emotion model,[17] which connects environmental stressors to negative emotions to aggressive behaviors, and the Organizational Citizen construct,[18] which captures in this case behaviors that reflect employees' lack of commitment to the organization and its processes. Lualhati and McGarvey also listed Situational Triggers that can ignite behavior by increasing individual stress. (See Figure 5.) Using a diagnostic methodology similar to the DSM-5, they suggest relating these specific behaviors to the critical pathway – on the presumption that more numerous examples of these behaviors may indicate a higher probability of more severe malicious acts, particularly if stressing events accumulate. Connecting the behaviors with the CWB taxonomy may help guide workplace managers and assistance programs in developing remediation strategies.

CWB: STRESSOR – EMOTION				CWB: ORGANIZATIONAL CITIZEN				CWB: SITUATIONAL TRIGGERS			
Behavioral Family				Behavioral Family				Behavioral Family			
INDIVIDUAL MINOR	INDIVIDUAL SERIOUS	INDIVIDUAL MINOR	INDIVIDUAL SERIOUS	INDIVIDUAL MINOR	INDIVIDUAL SERIOUS	GROUP MINOR	GROUP SERIOUS	ENVIRONMENTAL MINOR	ENVIRONMENTAL SERIOUS	CORPORATE MINOR	CORPORATE SERIOUS
NONVIOLENT	***NONVIOLENT***	***VIOLENT***	***VIOLENT***	***NONVIOLENT***	***NONVIOLENT***	***VIOLENT***	***VIOLENT***	***MODERATING FACTORS***	***MODERATING FACTORS***	***MODERATING FACTORS***	***MODERATING FACTORS***
• Poor performance ratings • Late to work/ meetings • Poor quality work • Misuse of time • Misuse of resources • Not accepting feedback • Disgruntled • Incongruent work history • Unreported changes in personal history	• Falsifying employment data • Excessive absenteeism • Theft of information/ property • Time card fraud • Falsifying work related data • Exhibits paranoia attitudes • Disregard for authority • Excessive secrecy • Distrust of others	• Unsafe behavior (risk taking) • Drug use • Alcohol use • Bullying of co-workers • Verbal abuse/ profane language • Unexpressed anger • Aggression towards others • Demonization	• Open anger • Destruction of property • Assault • Theft • Increasing paranoia • Actions dangerous to self and others • Disregard for authority • Arrests	• Late to work • Poor quality work • Misuse of time • Misuse of resources • Distrust outside of group • Loyalty shift from corp to group • Secrecy within group	• Absenteeism/ sick outs • Questionable group activity • Work slow down • Organized theft • Falsifying data • Distrust of outsiders • Demonization of non-group members/ organization	• Sick outs • Bullying outside of group • Unapproved meetings • Misuse of resources • Distrust outside of group • Loyalty shift from corp to group • Misuse of time	• Falsifying data • Unusual work patterns • Riots • Assaults • Sabotage • Organized theft • Open aggression to non-group members	• Medical issues (self/family) • Depression • Being bullied at work • Injustice (self or others) • Financial losses • Reward system • Job satisfaction shift • Suicide in family	• Loss of control (real or perceived) • Poor work relationships • Marital/ family difficulties • Poor job ratings • Passed over for promotion • Pending termination • Mal-assignment	• Practice vs. policy • Inconsistent selection process • Lack of training • Mal-assignments • Distrust of employees • Reward system changes • Ignoring security rules • Inconsistent reward process • Perceived authority shift	• Change of employee authority • Layoffs • Furloughs • No communication • Benefit loss • Employee treatment (loyalty) • Patronage (security/ promotion) • Terminations • Ethics violations

Figure 5: Initial Taxonomy of Families of Counterproductive Behaviors and Triggers Relating to Insider Threat

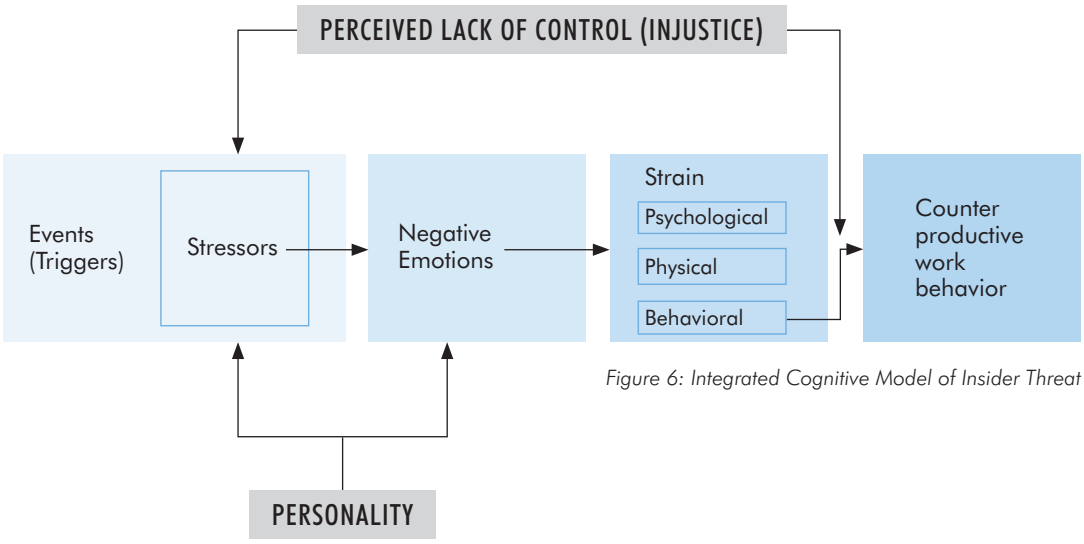

Figure 6: Integrated Cognitive Model of Insider Threat

AN INTEGRATED MODEL

The key studies cited use differing perspectives and data points but arrive at a similar conclusion – there is a timeline to major malicious acts from formerly trusted insiders. Assuming that individuals were loyal at the time of recruitment and hiring, they do not transform overnight from trusted insider to malicious insider but undergo a progressive deterioration that has cognitive and behavioral components.

The research and examination of recent high-profile malicious insider acts also clarify the components and steps that lead to concerning behaviors by trusted insiders who are moving along the critical pathway to commit major malicious acts. Integrating these factors into a model (see Figure 6) takes account of the process by which events can trigger stressors that are related to the individual's personality characteristics and perceived sense of control. An individual's perceived lack of control can amplify feelings of being unjustly treated. Those negative emotions create psychological, physical, and behavioral strains that can result in counterproductive work behaviors and ultimately a major insider act.

STANDING UP A BEHAVIORAL APPROACH TO INSIDER THREAT

Government, industry, and academia need to further test the plausibility and validity of using behavioral approaches to identify and mitigate insider threat. A solid understanding of the behaviors that lead to malicious insider acts is essential to translate theory into practice and develop measures to identify and mitigate behaviors before they become serious. Defining the clusters and families of measurable behaviors enables the creation of continuous evaluative tools to focus more quickly and effectively on critical concerning actions.

We caution, however, that understanding and addressing the causes of concerning and damaging behaviors require a focus on individuals and motives. Not everyone reacts the same way to specific situational stressors. Shaw, et al,[19] in studying IT system administrators, demonstrated that the interaction of individual characteristics and environmental factors that result in cyber-related damaging behaviors is complex, but predictable. This suggests that it may be worthwhile not only to establish an "early warning system" based on a behavioral approach to insider threat, but also to use this approach as a starting point for determining how individual characteristics (e.g. personality traits) and environmental factors either contribute to or mitigate concerning and damaging behaviors.

Both goals – improving early warning of vulnerability and understanding individual complexity – entail not only defining psychological models, but also seeking methodologies and tools that can assist in swift, continuous identification and assessment. Most efforts to date have focused on characterizing individuals at a specific point in time – during an initial or periodic investigation – but employers now recognize the importance of leveraging innovative technology and data sources to monitor and evaluate individuals on a continuous basis. Such ongoing scrutiny in no way substitutes for effective personnel security and counterintelligence processes; rather, it provides employers the opportunity to greatly enhance their ability to detect and divert insiders on the critical pathway to dangerous acts.

EXPANDING THE TOOLKIT TO ASSESS POTENTIAL MALICIOUS INSIDERS

Effective monitoring tools that can work in tandem with an integrated behavioral model must take advantage of new technology and go beyond the current standard that focuses on screening for biographic factors (i.e. criminal record, financial history) and the monitoring of computer and network activity. In particular, sophisticated psycholinguistic tools and text analytics can monitor an employee's communications to identify life stressors and emotions and help detect potential issues early in the transformation process.

> Three relevant tools to assess whether an individual may be moving toward a malicious act include personality mapping, life-event detection, and emotion detection.

In today's world, individuals are constantly tweeting, posting on blogs, sending emails, and texting. This explosion of social media data has correspondingly brought an investment in technology to analyze individuals based on their written and verbal words in everyday communications. Most of this technology was developed for retailers to better understand their customers and product preferences. Some of this technology is referred to as sentiment analysis or micro-segmentation for marketing purposes.

These same technologies can also be used to understand not just buying intentions, but general intentions toward any activity, including malicious acts. (Monitoring of email, social media, and other communications must be consistent with legal and regulatory requirements, organizations' internal policies, and other guidelines in ways that balance security requirements and employees' privacy rights.) Three of the most relevant tools to assessing the risk that an individual may be moving toward a malicious insider act include personality mapping (psycholinguistics), life-event detection (text analytics), and emotion detection (sentiment analysis).

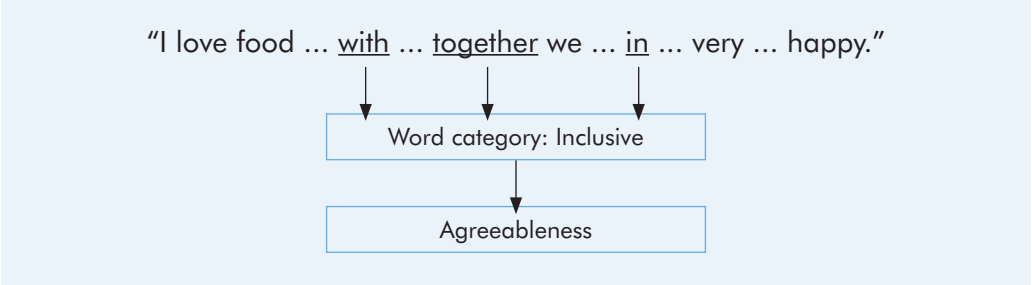

Figure 7: Psycholinguistic Mapping of Words to Personality Traits

PERSONALITY MAPPING

Psycholinguistic tools use linguistic analytics to extract a full spectrum of psychological, cognitive, and social traits from the data a person generates. By analyzing social media posts such as tweets, text messages, and emails, psycholinguistic tools can derive a model of an individual's Big Five[20] personality traits, values, fundamental needs, and emotional state. Personality mapping typically categorizes an individual's words and maps them to psychological categories that determine a certain personality trait, value, need, or emotion. For example, as shown in Figure 7, words such as "with," "together," and "in" map to the work category "Inclusive," which then corresponds to the personality trait "Agreeableness," which is associated with compassion and cooperation toward other people.

Some of these tools use linguistic analytics to extract a spectrum of cognitive and social characteristics from the text data that a person generates through blogs, tweets, forum posts, and email. They can generate scores relative to sample populations. For example, Figure 8 illustrates personality characteristics that were derived from Edward Snowden's posts to *Ars Technica*.

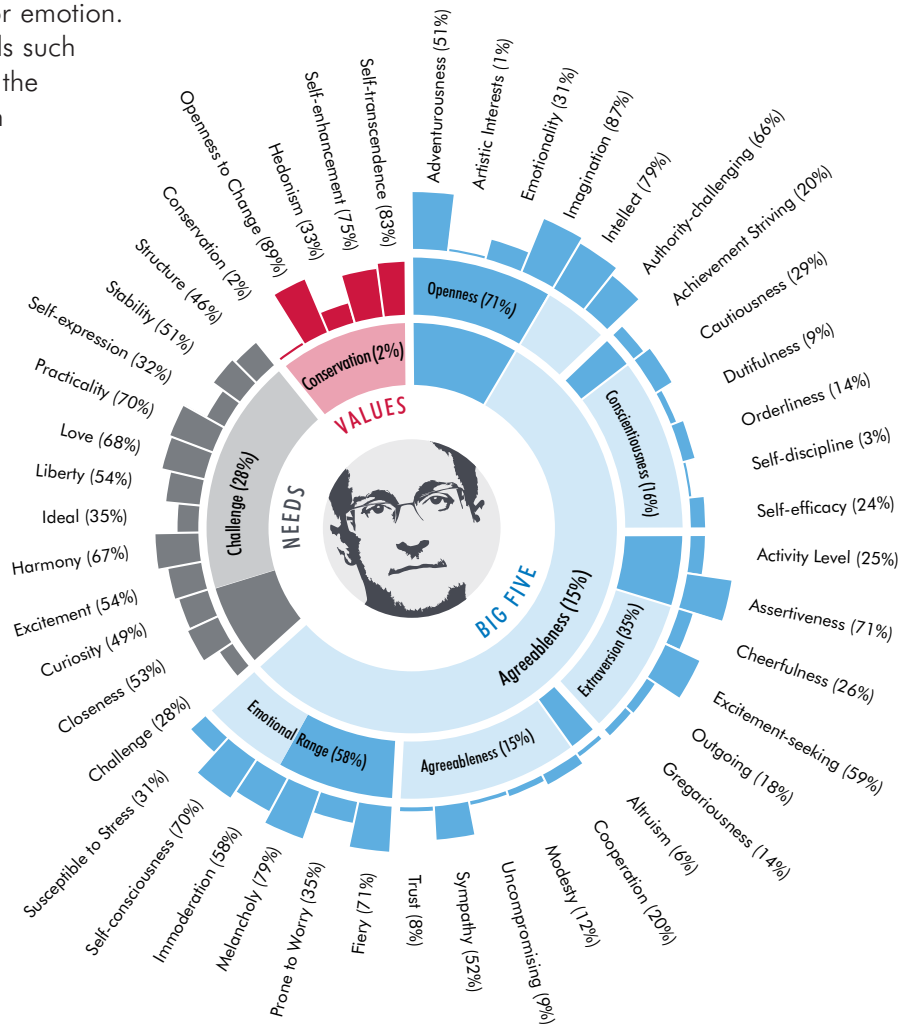

Figure 8: Characteristics Derived from Edward Snowden's Online Postings[21]

MODEL	PERSONALITY TRAIT	PERSONALITY TRAIT SCORE	CORRELATION	FINAL SCORE
Lack of Empathy	Altruism	6%	Negative	94%
Anti-Social	Gregariousness & Outgoing	14% & 18%	Negative & Negative	84%
Narcissism	Self-consciousness & Agreeableness	70% & 15%	Positive & Negative	77.5%
			Average Score:	**85%**

Figure 9: Alerts for Investigation Generated by Personality Mapping Tools

Within the personality trait of "Agreeableness," for instance, this tool can further refine the trait to "Altruism," "Trust," "Morality," "Modesty," "Cooperation," and "Sympathy." With this refinement, it can then map a personality portrait to insider threat models.

> Personality maps linked to insider threat models are smoke alarms, not smoking guns.

A very simple model of a malicious insider might look for characteristics such as lack of empathy, anti-social tendencies, and narcissism. A personality mapping tool (see Figure 9) can correlate lack of empathy negatively to "Altruism," anti-social tendencies negatively to "Gregariousness" and "Outgoing," and narcissism positively to "Self-consciousness" and negatively to "Agreeableness." If scores exceed pre-defined targets, tools can generate alerts for investigation and adjudication.

Personality maps linked to insider threat models are smoke alarms, not smoking guns. They can alert organizations to take a more careful look but are just one component of a full 360-degree view of a person's vulnerabilities that is informed by deep counterintelligence expertise. (See Figure 10.) The fact that most malicious insiders are narcissists does not mean all narcissists are malicious insiders.

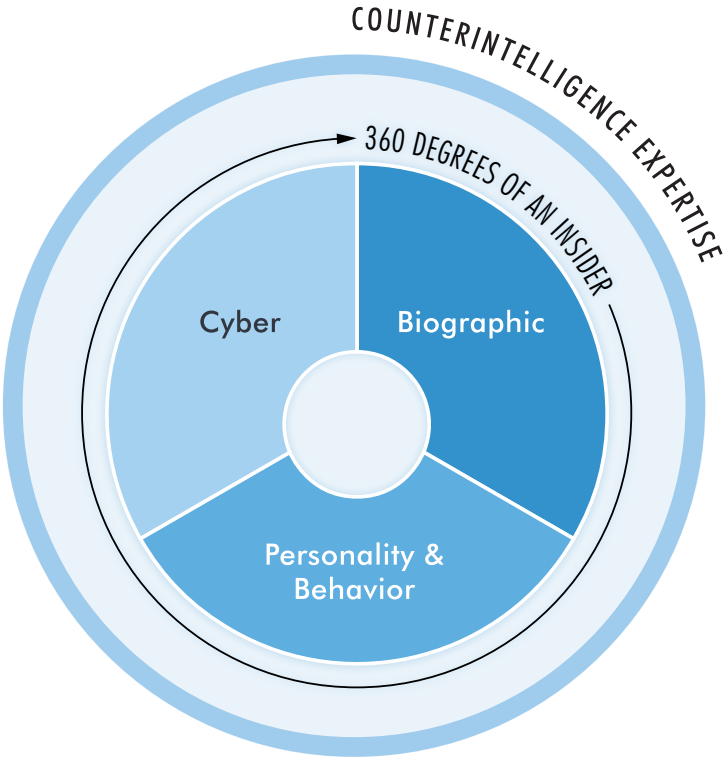

Figure 10: 360-Degree View of Vulnerabilities

Using Chelsea Manning's actual messages posted in an online instant chat, a typical live event detection tool would have extracted the following Key Words and linked them to the Life Event "Job End/Lost:"

> *(11:49:51 AM) bradass87:* and I already got myself into minor trouble, revealing my certainty over my gender identity... which is causing me to lose this job... and putting me in an awkward limbo

Life Event Key Word Found: job
Associated Words Near Key Word (within 3 words): lose
Life Event: Job End/Lost

A second blog post substantiates that Life Event and identifies an additional one, "Relationship End/Divorce" with two mentions for each Life Event:

> *(2:56:34 PM) bradass87:* my family is non-supportive... my boyfriend ditched me without telling me... I'm losing my job... losing my career options... I don't have much more except for this laptop, some books, and a hell of a story

Life Event Key Word Found: job, career
Associated Words Near Key Word (within 3 words): losing (2)
Life Event: Job End/Lost

Life Event Key Word Found: family, boyfriend
Associated Words Near Key Word (within 3 words): non-supportive, ditched
Life Event: Relationship End/Divorce

Life event tools combined with risk modeling software could correlate Chelsea Manning's multiple postings about negative life events to a significantly increased risk of undertaking a malicious insider act.

Figure 11: Life Event Linguistic Analysis of Pvt. Chelsea Manning's Email Postings[22]

LIFE EVENT DETECTION

A number of technologies, such as Natural Language Processing (NLP) and dictionary/rules-based text extraction, can detect life events. Tools using these technologies have been able to analyze social media data effectively, detecting not only life events but also emotional changes immediately following the event.

The explosion in use of social media sites such as Twitter, Facebook, Instagram, and Tumblr has led to the development of data mining tools and techniques to extract information from them. In particular, some focus on mining the data to understand more about what events are occurring. News organizations and Wall Street are particularly interested in understanding world events as they happen in real time, and retailers want to understand their customers' personal life events to tailor product marketing.

A variety of algorithms and techniques – including both rules-based (such as word dictionary look-up tables) and machine learning-based (such as Naïve Bayes, Support Vector Machine, Latent Dirichlet Allocation, and Bag-of-Words) – have been used to increasing effect in detecting life events. Some techniques are reaching 90 percent accuracy in correctly identifying a personal life event from an individual tweet, email, or blog. (See Figure 11.)

EMOTIONS DETECTION

Detecting emotional changes immediately following a life event is critical in understanding if a person is experiencing significant stress as a result of the event. Some tools can capture the common words used in the months preceding and following a life event and use them to help determine an individual's emotional state and the extent of emotional change. Detecting emotional change immediately following a life event is critical to understanding the individual's level of stress and to potentially developing mitigation strategies before unproductive and possibly malicious activity.

Sentiment analysis has also been effective in detecting life events such as the end of a significant relationship or a divorce, job promotion, being passed up for job promotion, death, illness, surgery, involvement in a lawsuit, travel, or graduation and then measuring the stress or corresponding change in emotion after the life event.

Through the use of machine learning (ML), the common words used in the months preceding or following a life event can be captured and a profile developed that can detect life events and corresponding stress just by the words the individual uses even if the life event itself is not mentioned. If individuals passed up for promotion use words or phrases right after the event such as "mad," "unjust," "revenge," "they don't understand," "idiots," "quit," and "I can't believe it," ML can help determine if a future spike in use of those words indicates a significant event, even if NLP or dictionary/rules-based text extraction tools fail to detect it. The tools can not only analyze the words being used but also to compare them over time and to use by peers within their organization.

ISSUES FOR DISCUSSION

An enhanced Continuing Evaluation process that anticipates malicious insider acts will, like any change, present issues to be considered and options weighed before deciding on the optimal course of action for the time, circumstances, and resources available. We anticipate the need for full discussion of issues such as the following:

> Through use of machine leaning, a profile can be developed that can detect life events even if the life event itself is not mentioned.

BALANCING PRIVACY AND SECURITY

Use of these tools entails extreme care to assure individuals' civil or privacy rights are not violated. Each organization must determine which employees should be exposed to psycholinguistic tools. One option is to only use these tools after behavioral observations have provided sufficient justification.

Only authorized information should be gathered in accordance with predefined policies and legal oversight and only used for clearly defined objectives. At no point should random queries or "What If" scenarios be employed to examine specific individuals without predicate and then seek to identify anomalous bad behavior. A successful insider threat program baselines authorized rules and triggers to be used against an entire population, including full-time employees, contractors, temporary employees, and former employees who retain access. This is particularly important for "about to be former employees," who might be anticipating Reductions in Force or layoffs.

A good starting point is to create baselines of employees' behaviors as they compare across job functions and peers that would reflect the organization's expectations for normal employee behavior. This enables measurement of baseline shifts, the sensitivity of which can be dialed up or down based on false positives. Acting on an incorrect identification of an employee as struggling and as posing a potential threat – a false positive – will erode confidence in the program and undermine employee morale.

IMPROVING ORGANIZATIONAL COMMUNICATION

The National Industrial Security Program Operating Manual (NISPOM) now requires industry to have responsible senior focal points for insider threat. This requirement not only facilitates interaction between government and industry, but also highlights the program's importance and ensures executives are briefed on improvements. Senior leaders' support and willingness to lead by example – specifically by agreeing to be monitored in the same manner as all employees – will improve the sharing of information among all involved components, including personnel, IT, legal, security, and management.

Employees deserve to be regularly informed of the dangers, indicators, reporting procedures, and consequences from insider attacks. Behavioral indicators, such as those discussed in this paper, should be transparently communicated to employees. The program's success depends on their participation in observing and reporting concerning behaviors on the part of their co-workers. They should be provided with a variety of means of reporting, which might include an option to report suspicious behaviors anonymously.

Equating organizational wellness with employee wellness will help convince employees that sharing information about a co-worker's odd or suspicious behaviors could help that person get support to resolve a life crisis. Employee assistance programs should be well known within the organization, effectively managed, and closely tied to the insider threat program.

FOCUSING ON AWARENESS AND MITIGATION

Employee assistance, insider threat, management, and all employees play important roles in mitigating problems before an employee goes rogue. Failure means lost lives, lost productivity, and financial cost. Caring enough to help employees through hard times will likely eliminate many incidents and in the end prevent loss.

Employees deserve to be regularly informed of the dangers, indicators, reporting procedures and consequences from insider attacks.

People are reluctant to disclose serious life stresses because they fear repercussions and career damage. Postmortems of past insider malice show a trail of lesser inappropriate or uncharacteristic acts that were not dealt with by the organization or by line managers. Psycholinguistic tools to help alert managers for the need for intervention will not take the place of better training and communication on the part of employees and managers regarding sets of behaviors and options for response.

> Effective risk management incorporates oversight and protections for privacy and civil liberties.

Having clearly defined processes in place before an incident is critical for successful mitigation. Implementing insider threat programs is most challenging for medium to large organizations because change takes time, money, and persuasion. Analyzing the information from new tools can be time consuming and require hiring new employees, which could be a challenge for small organizations and create resistance in fiscally constrained environments. In the end, it is cheaper to mitigate threats up front rather than lose millions of dollars and experience years of damage because of inadequate security processes.

PRACTICING RISK MANAGEMENT

Effective insider threat programs need to be based on solid risk management practices. Once in place, they need to be enhanced by broadening the scope of which employee aspects are analyzed to determine if they are a risk to the organization. Some refer to this as a "360-degree view of a person," a "whole person review", or "Risk 360" to indicate it is more than just cyber forensic logging and auditing.

Analyzing behavioral and psychological indicators provide a more complete view of the threat so it can be better managed and mitigated. Risk management is facilitated by proper models and tools that can assist human assessment and resource prioritization by measuring and ranking the amount of risk assigned to each person.

Effective risk management incorporates oversight and protections for privacy and civil liberties. An effective mitigation approach advocates the shifting or repurposing of existing assets to efficiently support the organization's strategic goals. It also embeds mitigation strategies and feedback mechanisms to deal with the insider threat and aims for a clear return on investment.

RECOMMENDATIONS FOR NEXT STEPS

Government and industry can work together on procedures and tools to anticipate and mitigate malicious insider acts. This process – like all successful security programs – must be adaptable but universal; accessible but adequately secure; and actionable but still timely and cost-effective. We make the following recommendations to integrate behavioral models, employee management, and new technology to identify and mitigate insider threats before they progress down the critical path to malicious acts.

1. *Share and refine the vision.* The INSA Security Policy Reform Council will seek partners in government and industry to determine interest and options for refinement and implementation of a comprehensive approach to mitigating insider threat. The concepts in this paper are not new but simply adaptations of existing research and its linkage to developing technology. Our reading is that these models and tools are readily compatible with current planning for insider threat, credentialing, and other security reform efforts and should be incorporated in them. We will track responses to this paper and encourage the integration of improved models and technologies to mitigate the insider threat.
2. *Clarify authorities, roles, and policies.* The authorities and roles of security, human resources, and information technology in thwarting malicious insiders are not clearly scoped. Implementing the concepts in this paper requires better definitions of roles and responsibilities and their reflection in policy. The ubiquity of IT has helped bring the stovepiped specialties closer together, but the effectiveness of the partnerships varies across organizations. We anticipate this paper will provide a platform from which to generate momentum for improved collaboration and clarification of roles.
3. *Validate the model, data sources, and tools.* Implementing these ideas requires a serious effort to validate that behavioral models and tools work as intended and that the data collected meets expectations. This entails strong government-industry partnerships to assess the inputs and outputs for legality, accuracy, and efficiency.
4. *Plan ahead for training adjudicators, analysts, managers, and employees to do business differently.* Conceptual models and automated tools can guide us to do what we should have been doing all along: helping struggling employees off the critical pathway to harmful actions. But in the end, people must recognize the leading behavioral indicators and act. This requires ensuring they have the analytic thinking skills to use machine-generated insights and to interpret behaviors observed in the workplace.
5. *Seek better solutions.* Government and industry have learned the hard way that our best attempts at planning will be overcome by the swirling pace of change. Any actions to respond to insider threat should anticipate that we must always seek to expand our understanding of people, improve our processes, and make more effective use of technology. Thoughtfully defined and scoped projects, data protocols, and spiral development are proven mechanisms for dealing with a shifting landscape.

ENDNOTES

[1]*Suitability and Security Processes Review, Report to the President, February 2014, 14. Available at https://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.*

[2]*Intelligence and National Security Alliance, Leveraging Emerging Technologies in the Security Clearance Process, March 2014. Available at http://www.insaonline.org/i/d/a/b/LeveragingTechnologies.aspx.*

[3]*Intelligence and National Security Alliance, Preliminary Examination of Insider Threat programs in the U.S. Private Sector, September 2013. Available at http://www.insaonline.org/i/d/a/b/InsiderThreat_embed.aspx.*

[4]*E.D. Shaw, K.G. Ruby, and J.M. Post, Insider Threats to Critical Information Systems: Characteristics of the Vulnerable Critical Information Technology Insider (Washington, DC: Political Psychology Associates, 1998).*

[5]*E.D. Shaw, K.G. Ruby, and J.M. Post, Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, and Recommendations (Washington, DC: Political Psychology Associates, 1999).*

[6]*Shaw, et. al., 1999.*

[7]*David L. Charney, "True Psychology of the Insider Spy," Intelligencer: Journal of U.S. Intelligence Studies (Fall/Winter 2010): 47-54. Available at https://www.ncsc.gov/issues/docs/Charney-PsychologyofInsiderSpyAFIO-INTEL_Fall-Winter2010.pdf.*

[8]*Jerrold M. Post, "Anatomy of Treason," Studies in Intelligence, 1975. (Declassified February 12, 1998).*

[9]*Paul R. Sackett, and Cynthia J. DeVore, "Counterproductive Behaviors at Work," in Handbook of Industrial, Work & Organizational Psychology, Volume 1: Personnel Psychology, edited by Neil Anderson, Deniz S. Ones, Handan Kepir Sinangil, and Chockalingam Viswesvaran (London: SAGE Publications, 2005): 145-164.*

[10]*Many articles discuss ways to frame the study and understanding of organizational misbehavior. See, for instance, Yoav Vardi and Yoash Wiener, "Misbehavior in Organizations: A Motivational Framework," Organization Science, Vol. 7, No. 2 (March-April 1996): 151-165. Available at http://home.ubalt.edu/NTYGMITC/642/Articles%20syllabus/vardi%20%26%20Weiner%20Misbeh%20.pdf*

[11]*E. Kevin Kelloway, Lori Frances, Matthew Prosser, and James E. Cameron, "Counterproductive Work Behavior as Protest," Human Resource Management Review, Vol. 20 (2010): 18-25. Available at http://ohpsychology.ca/wp-content/uploads/2011/02/Kelloway-Francis-Prosser-and-Cameron.pdf.*

[12]*Joseph Lualhati and D. McGarvey, "Developing an Insider Threat Program: An Integrated Insider Threat Behavioral Model" (presented at ASIS International Conference, Chicago, IL, September 24-27, 2013).*

[13]*The DSM-5 is the latest version of the American Psychiatric Association's classification and diagnostic tool, which is used in the United States as a key reference for psychiatric diagnosis. American Psychiatric Association. Diagnostic and Statistical Manual of Mental Disorders, 5th ed. (Arlington, VA: American Psychiatric Association, May 18, 2013).*

[14]*Eric L. Lang and Olga G. Shechter, "Improved Assessment of Personality Disorders that are Security Risk" (presented at the International Applied Military Psychology Symposium (IAMPS), Vienna, Austria, May 25, 2011).*

[15]*Olga G. Shechter and Eric L. Lang, "Identifying Personality Disorders that Are Security Risks: Field Test Results," PERSEREC Technical Report 11—05 (Monterrey, CA: Defense Personnel Security Research Center, September 2011). Available at http://www.dhra.mil/perserec/reports/tr11-05.pdf.*

[16]*Director of National Intelligence, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," Intelligence Community Directive 704, October 1, 2008. Available at https://www.dni.gov/files/documents/ICD/ICD_704.pdf.*

[17]*Suzy Fox and Paul E. Spector, "The Stressor-Emotion Model of Counterproductive Work Behavior." Counterproductive Work Behavior: Investigations of Actors and Targets, ed. Suzy Fox and Paul Spector (Washington, DC: APA Press, 2005).*

[18]*The Organizational Citizen construct, defined by Dennis Organ in the 1980s, describes behaviors that are outside of formal job descriptions and therefore difficult to define operationally. Researchers are tending to conclude the constructs are separate but related: organizations should encourage employees to engage in the enhancing behaviors and discourage counterproductive behaviors. For instance, see Reeshad S. Dalal, "A Meta-analysis of the Relationship between Organizational Citizenship Behavior and Counterproductive Work Behavior," Journal of Applied Psychology, Vol. 90, No. 6 (November 2005): 1241-1255. Available at http://dx.doi.org/10.1037/0021-9010.90.6.1241.*

[19]*Shaw, et. al., 1999.*

[20]*The Big 5 personality traits are often listed under the acronym OCEAN: Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism.*

[21]*This graphic was generated by "Personality Insights," an IBM Watson application, at https://watson-pi-demo.mybluemix.net/.*

[22]*Chelsea Manning's chat logs were obtained by Wired Magazine in 2010. See Evan Hansen, "Manning-Lamo Chat Logs Revealed," Wired, July 13, 2011. Available at https://www.wired.com/2011/07/manning-lamo-logs.*

ABOUT THE SECURITY POLICY REFORM COUNCIL

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

ABOUT THE INSIDER THREAT SUBCOMMITTEE

This subcommittee of the Security Policy Reform Council (SPRC) seeks to inform the U.S. Government and the private sector on best practices related to counterintelligence and insider threat, both in terms of late-breaking and longer-term issues. The subcommittee also provides a venue for collaboration through events, meetings and presentations. Contributing members come from companies and organizations at the forefront of cybersecurity, risk management, counterintelligence and big data analytics.

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions. As a nonprofit, nonpartisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities. INSA has over 160 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

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