

NOIR WHITE PAPER PART THREE

SERIES ON INSIDER THREAT/COUNTERINTELLIGENCE/COUNTERESPIONAGE

PREVENTION THE MISSING LINK

For Managing Insider Threat
in the Intelligence Community

*Counterintelligence is the Stepchild
of the Intelligence Community*

Prevention is the Stepchild of Counterintelligence

Detection Gets All the Love

Dr. David L. Charney
Psychiatrist

ABOUT THE AUTHOR

David L. Charney, MD



Dr. Charney is the Founder and Medical Director of Roundhouse Square Counseling Center, in Alexandria, Virginia. He specializes in Anxiety and Mood Disorders, Couples and Family Therapy, as well as Attention Deficit Disorder in adults.

In addition to his usual practice, he has also treated personnel from within the Intelligence Community. As a result of unusual circumstances, he had the opportunity to join the defense team of his first spy case, Earl Pitts. Subsequently, Plato Cacheris, the attorney of Robert Hanssen, invited Dr. Charney to join his defense team, which added a further dimension to his experience. With the addition of his third spy case, Brian Regan, Dr. Charney further deepened his knowledge of the psychological nuances of captured spies.

As a member of their defense teams, Dr. Charney was perceived by these insider spies as an understanding and supportive figure, which lowered their defensive mindsets, and provided a truer picture of their inner lives. Many common assumptions of spy motivation were brought into question by Dr. Charney's work.

Dr. Charney elaborated his findings in Part One of his White Paper, entitled *True Psychology of the Insider Spy*. Part Two of his White Paper, entitled *NOIR*, lays out Dr. Charney's innovative and perhaps controversial recommendations for making use of what he learned to better manage the problem of insider spies. To educate and promote these concepts and ideas, he founded NOIR for USA, a non-profit organization. Its website is: NOIR4USA.org.

PREVENTION: THE MISSING LINK

For Managing Insider Threat in the Intelligence Community

*Counterintelligence Is the Stepchild
of The Intelligence Community*

*Prevention Is the Stepchild of
Counterintelligence*

Detection Gets All the Love

Dr. David L. Charney
Psychiatrist

TABLE OF CONTENTS

Proposing a New, Comprehensive Strategy to *Prevent*, Not Detect, Insider Threat in the US Intelligence Community (IC)

SECTION A	1		
The Problem: The Insider Threat	1		
Analyzing Failed Links in Security Chains	1		
Missing Links in IC Security Chains: Off-Ramp Exits	1		
Disclaimer	1		
SECTION B	2		
Scope of the Problem	2		
Importance of Prevention Despite Its Neglect	2		
Overly Focusing on Detection at the Expense of Prevention	2		
Great Hopes of the Moment	2		
Dirty Little Secret of Counterintelligence (CI)	2		
SECTION C	3		
The NOIR White Paper Series on Insider Threat, Counterintelligence, and Counterespionage (CE)	3		
CHART: Ten Life Stages of the Insider Spy	3		
NOIR White Paper Part One	3		
NOIR White Paper Part Two	3		
NOIR White Paper Part Three	3		
The Vision: A Full Spectrum Solution for Managing Insider Threat	4		
SECTION D	4		
Rethinking Insider Threat	4		
External Management of Insider Threat (EMIT) vs. Internal Management of Insider Threat (IMIT)	4		
External Management of Insider Threat (EMIT)	4		
Internal Management of Insider Threat (IMIT)	4		
		Human Psychology is Central to IMIT-Based Prevention	5
		Situations of Concern	5
		Modern Sales Practices Are Key for Achieving “Left of Boom” Interventions	5
		CHART: EMIT vs IMIT	6
		Not New! IMIT-Based Approaches Already Practiced in Specialized IC Units	6
		Behavioral Change Stairway Model	6
		Full Spectrum Solution for Managing IC Insider Threat Requires EMIT and IMIT	7
		SECTION E	7
		Detection: Strengths and Weaknesses	7
		Detection: Core Mission of Traditional Law Enforcement	7
		Strengths of Detection	7
		Weaknesses of Detection	8
		Factors Contributing to Detection Weakness	8
		Intrinsic Weaknesses	8
		Workplace Barriers That Thwart Detection	8
		Workforce Hiring Paradoxes Within the IC	9
		Net Result of Detection Weaknesses	9
		Detection is Nearly Useless With “Whistleblowers”	9
		Problems in Execution	9
		False Negatives, False Positives, and Other Confusing or Bad Results	9
		Consequences	9

Looking Ahead: Excessively Optimistic Claims for New High-Tech Advances	10
Artificial Intelligence (AI), Big Data, Algorithms, and Machine Learning (ML)	10
Algorithm Bias: A Newly Named Concept	11
Paradigm of Home Security Systems	11
Thresholds in the Context of the IC	11
Defining Suspects Based on an Algorithm	11
An Insider Threat Score?	11
Arbitrary Thresholds Tend to Get Turned into Concrete Categories	11
Congratulations! You Identified a Suspect. Now What?	11
High-Tech Indicators: Helpful or Problematic?	11
Parallels the Problem of What to Do with Weather Forecasts	11
Bring in the Big Guns: The FBI Will Solve It!	11
Hassles Managing Suspects	12
Despite the Hype, High Tech Offers Little Relief for Decision Makers	13
Defeating the Newest Detection Technology? “Zero Days” Are Every Day	13
Big Picture Considerations: IMIT Advantages Over EMIT	14
Easier Decisions	14
Cheaper	14
Faster	15
Easier to Manage	15
Rescue vs. Catch	15

SECTION F	15
Prevention: Strengths and Weaknesses	15
Strengths of Current Practices	15
Weaknesses of Current Practices	15
Cultural: Prevention is the Stepchild of Counterintelligence	15
Measuring Success: Prevention’s Biggest Problem	16
Prevention Resources Today Need Strengthening	16
SECTION G	17
Building a New Comprehensive Prevention Program	17
General Considerations	17
IMIT Concepts Will Be Its Guiding Principles	17
Useful Starting Fact: About 90% of Insider Threat Actors Are Male	18
Intervention Windows: When Open and When Closed?	18
Introduction	18
First Open Window: Stage 2 (Stress/Spiral Stage): Before Someone Crosses the Line	19
Intervening During Early and Mid-Stage 2	19
Closed Windows: Stages 3 and 4: The Blackout Periods	19
Open Windows: Stage 5 (Remorse, Morning After Stage); Stage 6 (Active Spy Career Stage); and Stage 7 (Dormancy Stage): The Stages After Someone Crosses the Line	19
Two-Tier Structure Advocated for EAPs	19
First Tier: Existing EAPs Internal to Each IC Agency	19
Second Tier: A Second Level EAP – External to the Home Agency	20

Resources Must Be Real	20
An External EAP Has the Advantages of a Third Party	20
Resources	20
Making the New Prevention Program Work	21
Targeting the Correct Audience	21
Communicating the Right Way with the Target Audience	22
Packaging Offers	22
New Prevention Program Should Be Rolled Out in Phases	22
Phase One: Redefining the Meaning of Spying	22
Phase Two: Proving the Redefined Meaning of Spying	24
Phase Three: Getting the Messages Out	24
Locate Second-Tier Prevention Resources Under the ODNI	26
Best Practices	26
Employees Temporarily Immune to Prevention Messages	27
No Claim This New Prevention Program is a Perfect Solution	28
Legal Hurdles to Be Overcome	28
SECTION H	29
Conclusions	29
Detection is Necessary But Not Sufficient	29
Missing Links: Two Off-Ramp Exits	29
To Move “Left of Boom,” a Full Spectrum Solution is Needed	29
Final Message	29
ENDNOTES	30

PART THREE

PROPOSING A NEW, COMPREHENSIVE STRATEGY TO PREVENT, NOT DETECT, INSIDER THREAT IN THE INTELLIGENCE COMMUNITY (IC)

SECTION A:

THE PROBLEM: INSIDER THREAT

Recent dramatic security breaches have drawn increasing attention to the insider threat problem. These breaches have captured headlines and have featured perpetrators such as classic state-sponsored insider spies like the recent Chinese moles as well as so-called whistleblowers like Chelsea Manning and Edward Snowden.

My previous white paper, NOIR, proposed an off-ramp exit solution, which does not yet exist, for those who have crossed the line. Quoting Sun Tzu: “Always leave your enemy an exit.”¹ Extending the logic, why not off-ramp exits, meaning robust prevention mechanisms, for before they cross the line?

ANALYZING FAILED LINKS IN SECURITY CHAINS

Security breaches and other insider threat events are the endpoints that indicate a failure occurred somewhere along the sequence of links in security chains. These links are the protective measures intended to counter potentially disastrous breaches. Breaches are proof that the links failed.

Failed security chains in the IC should be analyzed the same way the National Transportation Safety Board (NTSB) goes about studying aircraft disasters. The NTSB seeks to understand how each link failed in chains that resulted in disasters and whether protective links that should have been built into security chains were simply missing.

MISSING LINKS IN IC SECURITY CHAINS: OFF-RAMP EXITS

This paper asserts that there are two critical missing links in IC security chains. These missing links can be described as two types of *off-ramp exits*: exits for *before* someone crosses the line and exits for *after* someone crosses the line. The absence of these two links in IC security chains weakens effective management of IC insider threat.

If both missing links were added to the considerable number of existing and planned detection links – which at present seem to be the only game in town – a *full spectrum solution* would come into existence for the comprehensive management of insider threat.

DISCLAIMER

Drawing attention to the shortcomings of detection does not mean that detection has little value for managing insider threat. Far from it. Detection is vitally necessary as one of the two key components of the classic *good cop-bad cop* dyad, universally employed for managing criminal offenders.

Every IC employee is on notice that a full range of detection methodologies continuously operate, creating powerful deterrence to not cross the line. With exciting new technological advances on the horizon, detection will continue to strengthen our national security.

That said, acknowledging the enduring and critical importance of detection should not keep us from exam-

ining its limitations. This paper will assert that there is an overreliance on detection, not that it is unnecessary. Currently, it is mostly bad cop and very little good cop, mostly stick and very little carrot.

While this paper will highlight many of the limitations of detection, my primary intention is to counter the IC's tendency to put nearly all of its eggs into the detection basket. Hopefully, critical thinking about detection will motivate the IC to reconsider relying so exclusively on it. The thesis of this white paper is that neglect of prevention strategies leaves too much on the table, too many opportunities to more effectively manage insider threat. Containing insider threat is too important to limit our toolset. We need more tools in the arsenal.

SECTION B

SCOPE OF THE PROBLEM

IMPORTANCE OF PREVENTION DESPITE ITS NEGLECT

The IC invests immense effort and resources into collecting, analyzing, and producing finished intelligence products, so it is demoralizing when insider threat events render them either useless or they wind up being used against us.

Prevention's importance is captured by the old sayings: "An ounce of prevention is worth a pound of cure" and "a stitch in time saves nine." Prevention is the one chance to head off disastrous insider threat events before serious damages are inflicted.

Despite that, prevention routinely suffers from neglect because it is not perceived to be as important as collecting and analyzing positive intelligence, or as compelling as detecting and catching insider threat actors red-handed in the act.

It is also fair to say that prevention, as currently practiced, has not been that successful.

OVERLY FOCUSING ON DETECTION AT THE EXPENSE OF PREVENTION

Newly hired IC employees are generally very carefully vetted, and only the most skilled, motivated, and patriotic prospects survive processing for clearance. Despite these strenuous efforts, very rarely, employees who started off good can turn bad.

Insider spies are different from professional hostile foreign intelligence entity (FIE) officers who, as their main aim, have the goal of penetrating our IC to steal our secrets from the very beginning of their employment.

To detect the bad actors, the IC has aggressively pursued innovative high-technology surveillance techniques and deployed and tightened up a full range of security measures. But what about what happens first, the mystery of why good employees turn bad?

Insider threat events originate within the minds of individuals. That is where it starts. Always.

Despite knowing that, relatively little attention has been paid to developing ways to shift the thinking of potential insider threat actors *before* they choose to cross the line.

The IC's strategy has been to mostly do what the IC knows how to do best – detection – not what is more needed to be done.

Prevention remains the weakest link in the IC security chain.

GREAT HOPES OF THE MOMENT

Great hopes have accompanied the rise of artificial intelligence (AI), big data, algorithms, and machine learning (ML), the bright shiny objects of the moment. There is a shared assumption that these high-tech innovations will introduce all that is necessary to finally resolve the challenging problem of insider threat.

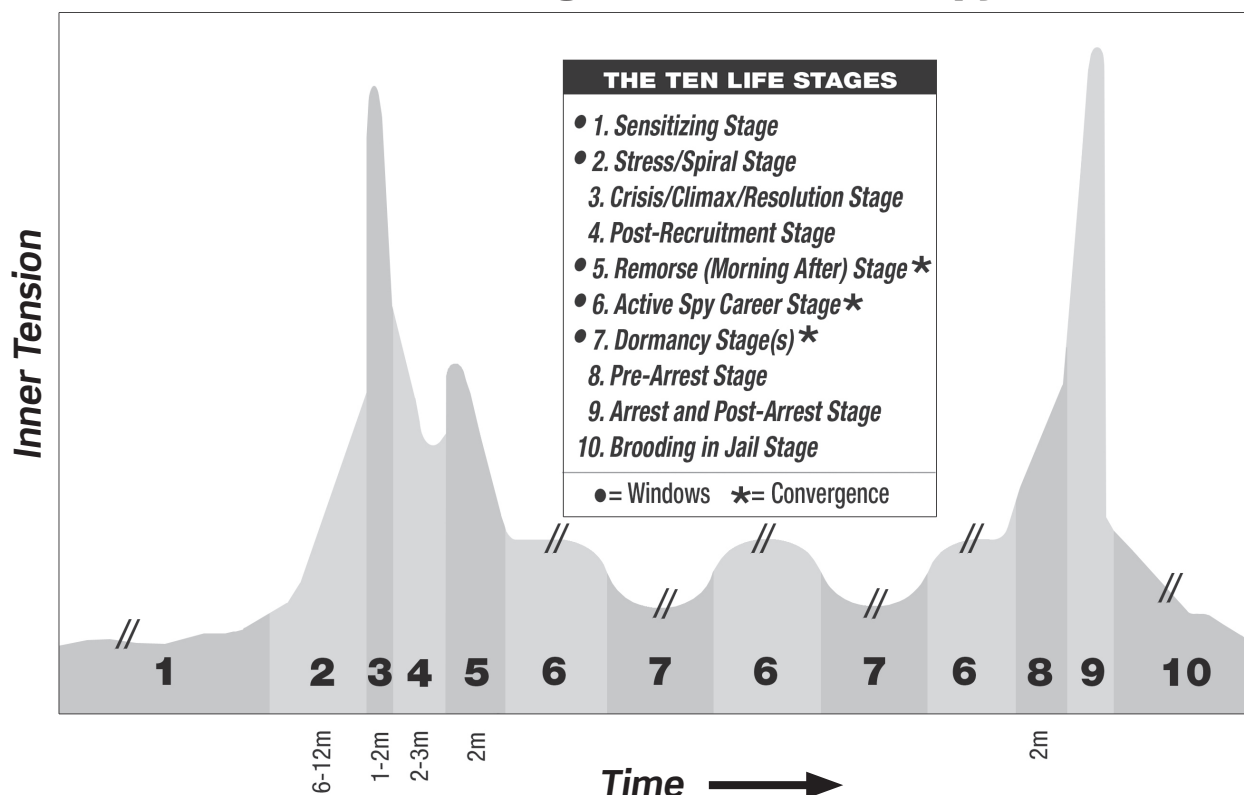
DIRTY LITTLE SECRET OF COUNTERINTELLIGENCE (CI)

Detection, for the attention it gets, has almost never caught any major spies. Nevertheless, somehow insider spies do get caught. How does it usually happen?

Nearly all major spy cases have been solved when someone from within the other side's intelligence service (i.e., the KGB) decided to cross over to our side, bearing *gifts*. To prove their *bona fides*, they brought over the names of IC employees their service were handling or enough key information that pointed to these traitors in our midst. As a result, some major spies eventually do get caught. However, the way they get caught is why detection cannot claim that much of the credit.

Giving credit where it is due, once insider spies do get identified as described, the FBI, in cooperation with other IC counterintelligence and security components, is quite effective doing what is necessary to close cases and get the offenders behind bars.

Ten Life Stages of the Insider Spy



©Copyright 2011 David L. Charney, MD

Advocates for modern amped-up detection methods claim that new and advanced technologies on the horizon will be game changers that will overcome the historical shortcomings of detection. I will explain why detection “on steroids” is not likely to move the needle that much.

SECTION C

THE NOIR WHITE PAPER SERIES ON INSIDER THREAT, COUNTERINTELLIGENCE, AND COUNTERESPIONAGE (CE)

NOIR WHITE PAPER PART ONE²

True Psychology of the Insider Spy addressed how to understand the fundamentals of the problem from the perspective of the psychology of the spy and the insider threat actor. This first paper introduced the concepts of the *Core Psychology of the Insider Spy* as well as the *Ten Life Stages of the Insider Spy*.

NOIR WHITE PAPER PART TWO²

NOIR: Proposing A New Policy for Improving National Security by Fixing the Problem of Insider Spies was intended to make practical use of my psychological findings. I proposed standing up the National Office for Intelligence Reconciliation (NOIR), essentially an off-ramp exit solution for *after* someone has crossed the line. NOIR would be a new mechanism to stop and then mitigate the damage our national security suffers due to uninterrupted espionage. I asserted that NOIR was a critical missing link in the IC security chain. Admittedly a controversial proposal, I knew NOIR could not be the entire solution on its own. NOIR did not adequately address a more important antecedent missing link in IC security chain failure: *How to prevent someone from crossing the line in the first place?*

NOIR WHITE PAPER PART THREE

This paper will examine in detail the most important missing link in IC security chains: *prevention*. Although prevention mechanisms do exist within the IC, they are relatively weak. I will recommend ways to make prevention stronger and work better.

THE VISION: A FULL SPECTRUM SOLUTION FOR MANAGING INSIDER THREAT

My first two white papers addressed how to better understand insider threat actors, when and how to intervene to reduce insider threat, and what resources are missing to get the job done.

The major proposal of my second white paper, NOIR, was to build an off-ramp exit solution for those who have *already* crossed the line. While NOIR capabilities do not yet exist, NOIR's core concepts can be carried over to engineer prevention solutions that will be more effective than current practices. This third white paper will propose off-ramp exit solutions for the situation *before* someone crosses the line.

All three white papers focus thinking on how to create a seamless suite of resources, *a full spectrum solution* for better managing insider threat, to include off-ramp exits for *before* and for *after* someone crosses the line.

SECTION D

RETHINKING INSIDER THREAT

EXTERNAL MANAGEMENT OF INSIDER THREAT (EMIT) VS. INTERNAL MANAGEMENT OF INSIDER THREAT (IMIT)

Introducing two complementary categories that advance a conceptual overview of insider threat management. For this discussion, insider threat actors, insider spies, and even “whistleblowers,” will be considered as somewhat interchangeable because in the early stages, these outwardly different actors demonstrate *strikingly similar underlying psychologies*.

EXTERNAL MANAGEMENT OF INSIDER THREAT (EMIT)

EMIT targets insider threat suspects with efforts that are externally focused, surveillance-based, intrusive, invasive, and even coercive. Detection is the principal discipline that epitomizes EMIT. Detection has always been law enforcement's primary means of managing criminal threat.

EMIT involves active and continuous surveillance of the entire IC workforce, scrutinizing a broad range of external, outside indicators to figure out what is going on inside.

EMIT's challenge parallels the children's book *Where's Waldo?*³ Within a vast crowd of good, law-abiding employees, there's a Bad Waldo: Find him! Detect him, catch him red-handed if possible, arrest him, prosecute him, and throw him in jail!

EMIT detection methods work to identify persons of concern by discovering behavioral indicators that hint of an inclination to cross the line or telltale indicators that someone has already crossed the line.

EMIT is based on what's done to subjects of interest. Suspects, known or unknown, are not offered the chance to cooperate and their permission is not requested. Rather, they are regarded as subjects to be hunted down. Clues are sought, behaviors observed, subjects are tracked until they are finally caught. Security measures and surveillance strategies can be adversarial, even antagonistic.

EMIT-inspired security measures include: Clearances; continuous evaluation (CE); repeat background investigations; polygraphs (polys); physical measures, such as fobs, passes, badges, Sensitive Compartmented Information Facilities (SCIFs), etc.; and mandatory procedural methods, such as passwords, biometrics, etc.

EMIT, from the warfighter's perspective, can be likened to air war: technical, prosecuted from a distance, remote, sterile, clean, abstract. However, though necessary and effective, air war is rarely able to win wars all by itself.

EMIT's consequences for suspects: When they get identified, what follows are adversarial confrontations; lawyers; prosecution; and ultimately, incarceration.

EMIT's attempts at prevention messages implicitly or overtly threaten and warn of dire punishments, delivered in authoritarian, sometimes scolding tones.

The IC almost exclusively relies on EMIT principles and has a limited appreciation for perhaps more important factors. The IC tends to lack sensitivity to the core psychology of insider threat actors, employees who are psychologically floundering, desperate, broken.

INTERNAL MANAGEMENT OF INSIDER THREAT (IMIT)

IMIT aims at changing the inner thoughts, attitudes, and mindsets of troubled IC employees to head off the worst developments, including crossing the line.

IMIT encourages IC employees to think about alternative ideas of how to manage their overwhelming life situations, which makes for healthier internal debate. Employees on the brink are persuaded to rethink their

dark, hopeless assessments and open up their minds to new, more positive ways of handling their problems.

IMIT attempts to convince employees to reach for helping resources that are presented as free choices. Resources would be attractively packaged for their due consideration.

IMIT is not based on law enforcement principles.

IMIT wants no part of an aversive, coercive, Stasi⁴-like workplace environment.

IMIT operates in accord with a softer, subtler “inner game” as opposed to a harder, more adversarial “outer

game.” As opposed to threats and warnings, offers of help are put forward.

IMIT, from the war fighter’s perspective, can be likened to ground war: close up and personal, one-on-

IMIT aims at changing the inner thoughts, attitudes, and mindsets of troubled IC employees to head off the worst developments, including crossing the line.

one, gritty, in-your-face. While benefiting from air war, ground war is the military arm almost always necessary to finalize conflicts to definitive conclusions.

IMIT requires no courts or lawyers, so there is more flexibility and maneuvering room.

IMIT saves time, energy, and money, including some of the expenses needed to prosecute, and incarcerate offenders. More important, IMIT interventions can head off disastrous treasonous acts along with the enormous costs that are associated with them.

IMIT sets up a very different, more cooperative transaction from the start, more of a problem-solving methodology.

IMIT’s key distinction: IMIT does not focus on catching hidden offenders. Rather, troubled employees are encouraged to come forward on their own. *They voluntarily self-identify.*

HUMAN PSYCHOLOGY IS CENTRAL TO IMIT-BASED PREVENTION

■ SITUATIONS OF CONCERN

Before (and after) the decision is made to cross the line, the situation should be viewed from the perspective of a male IC employee (females, far less frequently cross the line), who feels overwhelmed, stuck, trapped, unhappy, with no way out of his worst-ever life predicament. Desperation sets up his risk for making poor decisions like crossing the line.

LEFT OF BOOM

“Left of Boom” is a popular expression within the IC, referring to heading off a disastrous event, like an IED exploding, before it happens. When the chain of events is charted along a timeline, by convention, the bad end result is shown on the right side, so the antecedent events that led to the disaster are “left of boom.” Of course, far better to intervene “left of boom,” so the bomb never gets to explode.

■ MODERN SALES PRACTICES ARE KEY FOR ACHIEVING “LEFT OF BOOM” INTERVENTIONS

At its root, the insider threat actor’s problem is self-disappointment and loss of self-respect.

Taking this psychology of defeat and hopelessness into account is essential for accurately framing appeals.

IMIT-based offers derive their redemptive power from raising *hope*. Hope for rescue, for the chance to get a new start on life, for being able to snatch victory from the jaws of defeat. Potential insider threat actors, whether IC employees or cleared contractors, will be offered the option to take an off-ramp exit *before* making the decision to cross the line.

Soft sells as opposed to hard sells are the modern way. Employees can freely make their own choices to take the higher road. They will do so only if the rationales for choosing positive alternatives are safe, rational and well presented.

Solutions on offer cannot be viewed as demeaning. Honorable ways must be offered that restore self-respect. This can be achieved through respectful persuasion, not through messages presented in tones that are hostile, threatening, or coercive. Trying to engage hidden potential insider threat actors with accusative name-calling is a losing tactic. They are already in fight mode because that is their blueprint for trying to cover up their *intolerable sense of personal failure*. They are too well practiced with confrontation, so why fight a frontal engagement on their chosen turf?

Messaging must be aimed at meeting vulnerable employees where they are right now, “on the ledge.” They must be spoken to in terms that will penetrate their mental turmoil in simple, understandable language. Their crushed spirits must be understood and acknowledged. Give them what they are missing. In a word: *Hope*.

EMIT vs. IMIT

FACTORS	EMIT	IMIT
Professional Identity	Police	Sales
Spirit of Professionals	Hunters	Farmers
Actions	Catch	Persuade
Manner of Engagement	Doing <i>to</i>	Doing <i>with</i>
Type of Cop	Bad Cop	Good Cop
Carrots and Sticks	Sticks Only	Carrots Too
Warfare Type	Air War	Ground War
Emotional Tone	Cold	Warm
Sensitivity to Psychology	Minimal	Maximal
Concerns About Subject's Family	None	Major
Change Subject's Thinking?	No	Yes
Subject's Decision	Involuntary	Voluntary
Identified How?	Detection	Self-identified
Highest Aim	Punish	Save
Ideally, How It Ends?	Incarceration	Back to Work
Where?	Bureau of Prisons	Home Agency
Ancillary Professionals	Lawyers, Judges	Counselors

■ NOT NEW! IMIT-BASED APPROACHES ALREADY PRACTICED IN SPECIALIZED IC UNITS

Methods using softer appeals with dangerous characters in tough life-or-death situations are not new to the IC. These alternative approaches are well known, accepted, and practiced by specialized government units such as FBI hostage negotiation teams and police department special weapons and tactics (SWAT) teams.

Basic Strategy with Hostage Takers:

- Build a human relationship, a bonding
- Start a conversation
- Stretch it out, keep it going for as long as possible

- Delay rushing into action, do anything to decrease tension
- Suggest many alternative options
- Avoid getting confrontational
- Offer comfort items: food, calls to friends or relatives
- Do not jump to using guns, risking killing hostages or bystanders; use guns only *in extremis*.

■ BEHAVIORAL CHANGE STAIRWAY MODEL⁵

The FBI developed this model. Police negotiators who follow this model work through the following stages strictly in order:

- **Active Listening:** Understand the psychology of the perpetrators; let them know they are being listened to
- **Empathy:** Understand their issues and how they feel
- **Rapport:** When negotiators begin to understand how the perpetrators feel, they build trust
- **Influence:** Only when trust has been gained can solutions to the perpetrators' problems be recommended
- **Behavioral Change:** Perpetrators act more responsibly and may surrender

Important: Working through these steps in proper sequence is key. Do not try to effect behavioral change before rapport has been established.

This softer approach contrasts with older, more brute-force methods. In a parallel domain, for developing more effective interrogation techniques of captured terrorists, similar softer methods have evolved as the preferred approach.⁶

With insider threat actors, the hostage is not a person but rather the IC's precious classified national security secrets.

FULL SPECTRUM SOLUTION FOR MANAGING IC INSIDER THREAT REQUIRES EMIT AND IMIT

Detection approaches based on EMIT principles have been, thus far, the IC's nearly exclusive efforts to contain insider threat. Prevention, based mostly on IMIT principles, has been allocated far less thought and effort.

■ KEY POINTS:

- **EMIT-based detection is necessary but not sufficient**
- **IMIT-based prevention complements, does not replace EMIT-based detection**
- **Prevention addresses the situation before the decision gets made to cross the line, the most important missing link in the IC security chain**
- **Detection needs to be supplemented by adding off-ramp exit solutions**
- **Prevention provides the front-end off-ramp exit solution**
- **NOIR provides the back-end exit solution for after the decision gets made to cross the line**

■ GOALS OF THIS PAPER:

- To change the current situation, an almost exclusive reliance by the IC on EMIT
- To remedy the imbalance by adding IMIT tools to the arsenal

Comment on "Whistleblowers"

Proposals explored in this paper are designed to be effective not only with conventional state-sponsored insider spies but also with whistleblowers and other categories of insider threat actors.

SECTION E

DETECTION: STRENGTHS AND WEAKNESSES

DETECTION: CORE MISSION OF TRADITIONAL LAW ENFORCEMENT

Detection is at the core of the IC's DNA and has always been its most highly valued methodology. As mentioned, this is true despite what history shows: Detection has had only limited success in catching major spies. *Detection primarily focuses on finding employees who have already crossed the line but does not contribute much to keeping an employee from crossing the line in the first place.*

The IC has long experience and familiarity with detection approaches that come out of the world of law enforcement. Thus, detection operates right inside the IC's comfort zone. New proposals to improve detection usually amount to perpetuating the same timeworn practices, but promising to do them better, harder, faster, and amped up with modern high-tech tweaks. The newest proposals for improving detection do not capitalize on the expanded understanding of the psychology of insider spies and insider threat actors.

STRENGTHS OF DETECTION

Detection can provide early warning signals regarding employees of concern before they cross the line. In this respect, detection can overlap with prevention. Detection can identify malicious actors after they cross the line or at least can identify indicators of ongoing espionage.

Detection has always been the main approach for

managing insider threat precisely because it has demonstrated its many strengths since time immemorial. Detection strengths are so well known that listing them here in detail will add too much to an already lengthy paper. Highlighting an obvious point, detection's many strengths must be acknowledged.

WEAKNESSES OF DETECTION

■ FACTORS RELATED TO PRESENT DAY CONDITIONS

Exponentially Increased Risk Today

Classified documents are treated no differently these days than conventional documents: virtually all documents have shifted from paper to bits and bytes. Today, it is all zeros and ones. Massive amounts of classified material can be stolen using tiny thumb drives or other devices.⁷

More Hostile Foreign Intelligence Entity (FIE) Officers on the Prowl

Experts in the know state that more hostile FIE case officers are prowling around Washington today than during the height of the cold war.⁸ If stealing secrets is now so easy to accomplish remotely via the internet, why do our adversaries bother to work so hard at conventional human agent recruitment? Our adversaries would not be doing this if they did not see the value. Flooding the field with operatives, they will probably succeed in recruiting and handling as recruitments in place (RIPs) more of our IC personnel. It is partly a numbers game. Human intelligence (HUMINT) is still alive and well and often outperforms technical intelligence.

Generational Changes

The latest generation entering the workforce may be more self-absorbed, less loyal to their employers, feel more entitled and empowered to make decisions based on their convictions, and may be less attuned to the larger consequences of their actions. Consequently, the number of breaches seems to have increased.⁹

■ INTRINSIC WEAKNESSES

Detection is Subject to the Iron Law of Diminishing Returns

The costs of improving detection methods tend to increase more rapidly than results get improved. How much more investment of time, energy, and money will it take to improve detection outcomes? Hundreds of

millions of dollars to improve the catch rate of insider threat actors by only one or two percent?

■ WORKPLACE BARRIERS THAT THWART DETECTION

Coworkers find it hard to speak up.

No one wants to be a snitch! IC employees are reluctant to call out co-workers' behaviors of concern. Employees fear violating the culture of team spirit, trust, cohesion, sharing, and openness.

Moral reluctance.

Employees may feel it is presumptuous to assess and label others critically. That would be like casting stones. *Could I be next?*

Privacy concerns.

Employees do not want to cross lines of privacy and intrude into someone else's space.

Legal risks.

Suppose you are wrong? *Then what?*

Functional blindness.

This is the net result of these very human workplace barriers.

AN APPROACH THAT OVERCAME SIMILAR PROBLEMS: FAA STRATEGY TO DEAL WITH ALCOHOLIC PILOTS.

The FAA came up with a strategy to deal with the problem of alcoholic pilots. They knew other flight crew were reluctant to blow the whistle on alcoholic pilots because it might cost the pilots their jobs. They were afraid of being snitches.

The policy was revised to assure flight crews that if they did the right thing and turned in any alcoholic pilot, that pilot would not be fired. Instead, the pilot would be confronted and offered a chance to attend an aggressive alcohol treatment program. If they completed the program and its follow up treatment, they could fly again.

Sometimes a member of the flying public would hear about this program and be appalled: "You mean I could be flying with a recovering alcoholic pilot at the controls?!" The answer: "Would you rather be flying with an active alcoholic at the controls?"

Pervasive all-seeing surveillance regimes can backfire.

The atmosphere of ubiquitous surveillance degrades agency morale. Who wants to live in a workplace that resembles East Germany under the Stasi's omnipresent surveillance?

■ WORKFORCE HIRING PARADOXES WITHIN THE IC

IC's Claims About Its Ideal Hires

The IC ideally wants creative thinkers, unafraid to pursue new ideas, explore unusual sources, good at connecting dots, all in accordance with the vaunted post-9/11 lesson: "Beware the failure of imagination." Messy, complicated minds will be fine since they are useful for some aspects of analysis. The IC will have to grudgingly accept that private lives may be somewhat alternative.

What Really Happens? Paradoxical Results

With oppressive surveillance regimes, the qualities mentioned above would be discouraged. Different, imaginative, adventuresome types would be deselected or made unwelcome. They are too risky and dangerous! Oppressive work atmospheres are too constraining for these types – they will soon leave thinking: *Who needs it?* Oppressive surveillance regimes select for conventional, compliant, steady but unimaginative types, resulting in a workforce at the opposite pole from what was desired.

■ NET RESULT OF DETECTION WEAKNESSES:

Overly stringent detection surveillance regimes can cut two ways. Weighing security vs. competence, what is the right balance?

■ DETECTION IS NEARLY USELESS WITH "WHISTLEBLOWERS"

Detection may help if the potential whistleblower takes his time gathering his trove of classified materials so that his preparations may get noticed.

However, with impulsive actors moving rapidly, events can overtake detection methods. Sensitive materials can explode into public view with nothing left to detect!

Prevention, not detection, is the only way to head off whistleblowers.

■ PROBLEMS IN EXECUTION

"Solving" Problems: Appearances vs. Reality

Government tends to throw big money at tough problems for solutions that will not necessarily work. Senior management points with pride to closing new

"BIG IRON"

"Big Iron" was a term used by government contractors to describe massive hardware purchases, parts of the systems sold to the government that were claimed to solve incredibly complex problems. After tens or hundreds of millions of dollars were spent and nothing got solved, the machines were occasionally literally hidden away in the unhappy agency's subbasement to conceal the proof of the failure, thus hopefully sparing some of the embarrassment.

large contracts aimed at deterring insider threat. It shows "something is being done."

Contracts for developing and deploying complex new systems have long time horizons, subject to what one expert described as "The Conspiracy of Hope."¹⁰ Interested parties pretend that everything will work just fine, another Washington example of "the triumph of hope over experience." Despite initial grandiose claims, when mega projects show minimal success, or when they prove to be outright failures, disappointing results somehow seem to disappear. Who pays attention and tracks these long-term projects? By the time contracts get close to completion, the original government plank holders have retired. Contractors still embedded in a project may be aware of the program's shortcomings but have career and economic stakes in calling it a success.

Many Washington stories tell of enormously expensive projects that came to naught. It used to be called "Big Iron," hidden out of sight in the basement.

■ FALSE NEGATIVES, FALSE POSITIVES, AND OTHER CONFUSING OR BAD RESULTS

False Negatives

Failure to identify insider threat actors and their activities. They just do not show up on the radar.

False Positives

Misidentification of innocent employees as being malicious insiders or insider spies.

■ CONSEQUENCES

False positives adversely impact agency coworkers when they personally know the "suspect" and the allegations do not add up. They worry: *That makes no sense. Who will be caught the next time the music stops? Me?*

EXAMPLE OF A FALSE POSITIVE: BRIAN KELLEY

Brian Kelley was a true American patriot, possessing the highest level of professional integrity. Nevertheless, the FBI decided that he fit the parameters of a mole suspected to be operating within the CIA. Ironically, this was partly based on Kelley having solved the case of State Department Foreign Service Officer Felix Bloch. Kelley used his unique brand of detection analysis and solved one of the very few insider spy cases based on shrewd detection. Unfortunately, that success was twisted as evidence to be used against him.



There were other breathtaking errors, including finding a map at Kelley's house that was interpreted as locating drop sites in the park nearby. Except it was really Kelley's jogging map!

Kelley and his family were subjected to high pressure for over three years. Kelley never cracked, which was seen as further proof that he must be a *master spy*.

After a long ordeal, lo and behold, as it usually happens, a former KGB officer came over with information indicating that the spy was actually one of the FBI's own, Special Agent Robert Hanssen.

Washington is a surprisingly small town. Brian Kelly was my friend. How can one explain the amazing coincidence that Brian Kelley got suspected to be the spy that Robert Hanssen actually was? And that I wound up being the psychiatrist who worked with Robert Hanssen for a full year in jail after he was caught?

I listened to hours of hurt and pain Brian Kelley expressed to me from time to time. However, Brian took the high road and never sued the government. He just wanted to get back to his job in CIA counterintelligence and teach and mentor to the rising generation of new intelligence officers. He was appreciated and loved by his many students and protégés. Sadly, I believe the stress of it all led to his untimely death. False positives are *not* trivial!

These situations can degrade morale. Many employees are made chronically insecure, edgy, and nervous.

Personnel consequences can be expensive. Careers can be ruined when someone erroneously gets relegated to the penalty box. Losing highly selected, trained, and experienced personnel with not easily replicated specialized skill sets imposes high costs: to recruit, clear, hire, train, and replace key personnel. Also, it costs time to get back up to speed.

Frustrating Situations:

Example of the Felix Bloch Case

Bloch was known to be a spy. However, once he was alerted that he was under suspicion, he made sure not to get caught red-handed. Bloch fell into the non-prosecutable category. The IC's hands were tied. Now what?



- No solid confirmation of Bloch's spying
- Bloch could not be prosecuted
- Nothing was left to do
- The IC's last resort? Merely harassing Bloch
- The IC was left frustrated because the most valuable asset to be gained from a captured spy, a full damage assessment, was out of reach

LOOKING AHEAD: EXCESSIVELY OPTIMISTIC CLAIMS FOR NEW HIGH-TECH ADVANCES

ARTIFICIAL INTELLIGENCE (AI), BIG DATA, ALGORITHMS, AND MACHINE LEARNING (ML)

When examined more closely, advanced methods such as high-tech surveillance, AI, big data, algorithms, and ML are unlikely to deliver "slam dunks" regarding identifying insider threat actors or guiding what to do with alleged suspects.

AI, big data, algorithms, and ML operate autonomously and make decisions based on obscure algorithms employing unknown criteria, not necessarily based on anything resembling sound human judgment. This supposed advantage could conceal significant flaws.¹¹ Algorithms can contain hidden biases that distort results.

ALGORITHM BIAS: A NEWLY NAMED CONCEPT¹²

This refers to hidden biases built into algorithms, also called Unconscious Bias. Once baked in, there is no way to know what criteria were used to generate results. System designers tend to be reluctant to find and fix these biases. This revisits the computer world's perennial problem of garbage in/garbage out (GIGO). Lack of clarity and transparency regarding the obscure parameters that figure into machine-generated decisions means that findings can be just plain wrong, thus, easily challenged. Unfortunately, this can lead to bad judgment calls and follow-on consequences since the personal stakes are high for employees who come under suspicion. How much confidence can there be when the ML "black box" kicks out its conclusions? Right or wrong, findings can and will be challenged.

PARADIGM OF HOME SECURITY SYSTEMS

The art and science of setting threshold sensitivities of home security system window sensors demonstrates that *setting the sensor threshold is key*. If the threshold is set too high (insensitive), then even someone breaking in will not be enough to set off the alarm. If the threshold is set too low (overly sensitive), then any passing wind can set off the alarm. When police come the second time, they are annoyed. The *third* time, they may give you a fine.

THRESHOLDS IN THE CONTEXT OF THE IC

If thresholds are set too high, there will be false negatives and real cases will be missed. If thresholds are set too low, there will be false positives, with unfair and ruinous career consequences for innocent employees.

Also, an enormous number of employees are likely to come under suspicion so that impossibly large case-loads will now require clearance. All suspects will have to be processed, interfering with mission as suspects get sidelined during lengthy clearance reinvestigations.

There is no way to achieve a perfect threshold setting.

The only recourse: Determine an optimal threshold, based on tradeoffs and compromises, and then periodically readjust. Which is a nice way of saying it is not so much pure science as having to make *human judgment calls*.

DEFINING SUSPECTS BASED ON AN ALGORITHM

■ AN INSIDER THREAT SCORE?

Specific cutoff numbers, or segments of the population that raise concern? The software will determine the edges between different segments and will amplify edge contrast, sharpening small differences. Result: the illusion of precision.

■ ARBITRARY THRESHOLDS TEND TO GET TURNED INTO CONCRETE CATEGORIES

What began as reasonable theoretical models for defining "persons of interest" will get operationalized by bureaucracies into categorical guidelines that may not make real world sense. Imagine this conversation:

"Jim, I know you are a good guy, but the machine just told me you are a risk. I feel terrible about it, but for now, you have to leave our office."

CONGRATULATIONS! YOU IDENTIFIED A SUSPECT. NOW WHAT?

■ HIGH-TECH INDICATORS: HELPFUL OR PROBLEMATIC?

When the algorithm kicks out a precise numeric score, "a scientific assessment" that sharply meets the (arbitrary) threshold you or the machine set for defining insider threat concern, the issue promptly converts to a strictly human judgment call: *What do you do next, how do you handle it?*

■ PARALLELS THE PROBLEM OF WHAT TO DO WITH WEATHER FORECASTS

"Today, there is a 30 percent chance of rain."

Sounds very scientific. This seemingly precise percentage does not provide you with a clear answer to your practical question. It still falls to your judgment, your estimate of risk, and risk tolerance, as to what to make of the percent quoted.

Do you or do you not lug around your umbrella today?

■ BRING IN THE BIG GUNS: THE FBI WILL SOLVE IT!

Not so fast. Now another bureaucracy is in the decision mix with its lengthy timelines and obscure protocols. FBI Special Agents can have their own reasons to drag out investigations.

First, Special Agents are busy with other, perhaps genuinely more pressing matters.

Second, Special Agents become parties with their own interests. FBI personnel have their own stakes in the game, namely, protecting their own careers. Why risk reputation on behalf of an uncertain IC employee, when clearing that person may later prove to have been the wrong call? It is easier and safer to avoid clearing anyone who is remotely suspicious. The clearance process is not transparent so there is little risk attached to delaying or denying clearance. Who can challenge delays or outright clearance denials when the mysterious process hinges on unknown classified details?

When clearance decisions do not come quickly, other costs get imposed. As they say in legal circles: “Justice delayed is justice denied.”

■ HASSLES MANAGING SUSPECTS

- How will each risk segment be managed compared to the others? Why?
- What about someone on the boundary line between segments?
- How will individual suspects be handled?
- Direct interrogations? Secret investigations?

What if there are too many suspects to investigate?

There will probably be many false positives, which, as mentioned, can overwhelm the entire security clearance system. Consequences include sidelining too many key personnel, which can degrade fulfilling critical missions.

“FAILING THE POLY”: AN EXAMPLE OF HOW REAL-LIFE SITUATIONS GOT MESSY

How “failed polys” were handled:

Any result that was not a definite pass led to follow-up FBI investigations that could last for years.

Typical explanations that were given by security for sidelining employees: “We take many factors into consideration. The poly is just one tool.”

No, it wasn’t.

It was a career killer.

My experience with about a dozen CIA employees who “failed the poly”:

Not one stood out as a traitor.

Some were genuine heroes who sacrificed much for our country.

Nearly all had either hard life experiences that sensitized them, or had obsessional worry about minor or inconsequential details. In short, most were worrywarts who overthought things.

How were these problematic employees handled?

They were no longer “worldwide eligible,” therefore, they were no longer promotable. But they were retained in their current jobs, usually with continued access to classified materials. They were neither fish nor fowl. How confusing!

Sidelined employees typically chose to put up with their limbo status and stayed in their jobs because they had so much invested in their careers, and of course, they needed to protect their retirements. They were forced to “retire in place” well before their actual retirement date.

This created a class of hurt, disgruntled, angry, and bitter employees, the very class of employees you do not want to be working in your agency. This paradoxical result was the opposite of what was intended. Employees were transformed into the same reservoir of unhappy people from which insider spies get recruited!

Possible remedy: Change the threshold criteria?

Then it becomes even more transparently arbitrary and subject to challenge.

Confront, counsel, or hold back?

Damned if you do, damned if you don't.

You cannot ignore suspicious behaviors because that would implicitly give the green light for such an employee to keep doing his sketchy activities. If you do confront him, it can be the very trigger that causes the worst outcomes you most fear. What if a confrontation annoys or even outrages a suspect and becomes the very predicate for tipping him over to finally commit a treasonous act?

These are the “hot potato” scenarios, where you are damned if you do and damned if you don’t – the very problems that Judge William Webster identified as what kept him awake at night.¹³

DESPITE THE HYPE, HIGH TECH OFFERS LITTLE RELIEF FOR DECISION MAKERS

Results from high-tech surveillance findings do not relieve decision makers of the problem of what to do with the results, how to handle specific cases. Human beings, not machines or algorithms, still must make the hard decisions.

Clinton's Arkansas story

After winning his first presidential election, to explain how he now felt, Bill Clinton told his Arkansas story of the dog that chased a pickup truck all through town. When the dog finally caught up with the pickup truck, it had no idea what to do next!

It is the same thing when you identify an insider threat suspect. *Now what?*

DEFEATING THE NEWEST DETECTION TECHNOLOGY? “ZERO DAYS” ARE EVERY DAY

Determined insiders can and will defeat any security technology devised. It takes years and enormous cost to conceive and build advanced technology systems that are secure, with built-in detection components, which gives plenty of time for motivated hackers and insider threat actors to figure out how to defeat them. Also, after any such new system finally gets deployed, its details inevitably leak out. Determined insider threat actors will soon find a way to exploit them. Naïve insiders who try to breach these systems may get snared, but not the more sophisticated and dangerous insiders.

This situation resembles the age-old back and forth cycles experienced with any new “super weapon.” Soon after its deployment, the next advancement in defensive countermeasures neutralizes the latest super weapon. Then it recycles again and again.

Exceptions showing the best protections can be overcome

Ronald Pelton and Anna Montes were insider spies, but neither of them needed physical documents. They both had photographic memories and walked out with everything memorized!

What everybody in the information technology (IT) world knows

Someone in their mother’s basement anywhere in the world can penetrate the most secure computer system. Sophisticated IT experts no longer promise perfect protection from intrusions. They are resigned to the fact that any system can eventually be penetrated. They now talk about managing risk, making decisions of what to protect, with what levels of defense considering the costs, and how to build resilient capabilities to mitigate penetrations when they inevitably occur.

Cycle Times and OODA Loops

With massively complex high-tech security systems, as each new intrusion threat materializes, there is limited agility to devise protective fixes and workarounds. By the time a new fix gets fielded, hackers have moved on to exploit the next vulnerability they have already discovered. OODA Loop cycle times (“Observe, Orient, Decide, Act”) that are too slow will prevent getting ahead of the curve. Never a good night’s sleep for security experts!

OODA LOOPS

United States Air Force officer John Boyd developed the concept of OODA Loops.

I was introduced to Boyd’s ideas by a surprising source: the spy Robert Hanssen! This illustrates the complexity of human beings. On the one hand, Hanssen was a Russian spy. On the other hand, he regarded himself as a loyal American and tried to improve and strengthen the capabilities of the FBI, for which he worked.

Hanssen told me that he found no interest within the FBI to learn anything from Boyd. This rejection of Hanssen’s potentially valuable contribution to the FBI was yet one more hurt that added to his alienation.

Continuous Evaluation (CE)

The latest miracle cure, CE, proposes to rely on many of the high-tech detection activities described above. In theory, bad actors cannot avoid leaving a trail of breadcrumbs that will disclose their malicious behavior. These indicators will be picked up by any number of sensors, to include the latest internet of things (IoT) technologies.

We can comfortably assume that smart and well-motivated malefactors will quickly wise up about these technologies and adapt their behavior to operate under the radar. Strategies and tactics of how to defeat many of the newest technologies are staples of modern military thriller novels. If novelists can invent clever ways to evade or counteract any new, brilliant high-tech system, real insider threat actors will be even more motivated.

Example: Proving the Point

After briefing a CIA group, I met someone from the Directorate of Science and Technology (DS&T), who laughed when he heard about claims that were made re-

garding the latest, supposedly impregnable system. He told me: "Give me a few hours and I'll defeat any new thing you

"Give me a few hours and I'll defeat any new thing you put in front of me. I don't want to do it. But if I *did* want to do it, believe me, I *could* do it!"

put in front of me. I don't want to do it. But if I *did* want to do it, believe me, I *could* do it!"

Adding to the CE problems already discussed, extreme surveillance regimes can backfire by driving away the most desirable members of the future IC workforce. As prospective IC employees learn more about CE, they may get turned off and pass on ever applying for an IC job. Or if they do come on board, eventually out of sheer annoyance, they may decide to quit. Detection in the form of CE, while it may add more strength to deterring insider threat, may also turn out to be a cure that is worse than the disease. Once again, CE, like other detection methodologies, is a double-edged sword.

Message to Designers of Detection Systems, Including CE:

- You are smart, but you are not that smart
- Your adversaries are smarter
- They have all day to figure out how to beat your system

- You can never think of every which way to block their creative brilliance
- Read the news and learn about the latest penetration of any system you can name
- They are smarter. That is why you hired them in the first place

BIG PICTURE CONSIDERATIONS: IMIT ADVANTAGES OVER EMIT

EASIER DECISIONS

EMIT and detection methods make for difficult decision-making about insider threat suspects because they are grounded on the many uncertain, ambiguous premises mentioned above. IMIT mostly avoids these problems. IMIT makes life easier. There is no need to make hard calls based on imprecise indicators since IMIT is based on *voluntary self-identification*. Whether before or after crossing the line, the person of interest *shows up on his own*. Thus, no ambiguity.

Subjects who *voluntarily self-identify* simplify the problem because no elaborate detection efforts are required. Dangerous developments get short circuited earlier. That said, self-identified subjects must still be handled carefully and sensitively. By definition, they are still contending with major life stresses, still in a state of mental turmoil and overwhelmed by turbulent emotions.

CHEAPER

Standing up IMIT resources is less expensive than EMIT (but still not cheap).

IMIT cost accounting:

First, savings from scaling back some of the high costs of elaborate new detection systems can counterbalance some of the costs of IMIT. Of course, EMIT efforts must be kept robust since they will always be critically important. That said, overreliance on EMIT is the issue. The relative neglect of IMIT efforts needs to be addressed. Allocation of IC resources and effort has to be rebalanced.

Second, and most important, IMIT costs will be offset by stopping or mitigating major harms to our national security *that will never come to be*.

FASTER

Detection can take a very long time before subjects get identified. Since nearly all major spy cases do not get solved until someone from the other side crosses over to our side, the timing of that happy event is utterly unpredictable. While active counterintelligence and foreign intelligence recruitment in place (RIP) operations are always ongoing, it boils down to hoping something good will happen and happen quickly. *Hope is not a strategy.*

EASIER TO MANAGE

It is easier to manage voluntary, self-identified, relatively cooperative employees who turn themselves in, as compared to employees who were caught because of detection and who are now disappointed, fearful, and angry. Voluntary, self-identified employees are less likely to be vengeful and defiant. They are less liable to focus on the idea that the IC is their enemy. Since they chose to step forward on their own, they are more likely to recognize and admit to their deficiencies and poor choices, more likely to be ready to refocus on seeking paths to recovery.

IMIT approaches are supportive of an impaired employee's need to restore his sense of dignity, self-respect, pride, and manliness. He will take comfort from knowing that the IC recognizes and respects his real needs.

A troubled employee's core intention was probably never to harm the national security of the United States. His fundamental problem was mainly an internal personal crisis that played itself out in the workplace setting.

RESCUE VS. CATCH

In many cases, IMIT approaches will be able to save good employees who nearly went astray and return them to useful work.

SADLY, NOT EVERY TROUBLED EMPLOYEE WILL BE RESCUABLE

In which case, the proposed NOIR mechanism would be helpful to have already in place, ready as a backup option and alternative off-ramp exit solution, if needed.

SUMMING UP:

- ***IMIT confers advantages over EMIT for managing insider threat both before and after crossing the line.***
- ***EMIT still remains the bedrock foundation for robust multilayered defenses against insider threat.***

SECTION F

PREVENTION: STRENGTHS AND WEAKNESSES

STRENGTHS OF CURRENT PRACTICES

Prevention elements that do work well, often combined with elements of detection:

- Thorough initial vetting before hire
 - Security training during onboarding
 - Periodic reinvestigations
 - Repeat polys
 - Continuous technology-based surveillance
 - Physical security measures such as SCIFs, biometric identification, etc.
 - Routine security procedures, such as passwords, ID passes, fobs, two-person protocols, and numerous other EMIT security practices
-

WEAKNESSES OF CURRENT PRACTICES

■ CULTURAL: PREVENTION IS THE STEPCHILD OF COUNTERINTELLIGENCE

Detection is the preferred mindset of the IC. Just detection. Prevention runs against the grain, the DNA, of the IC. *Prevention gets no love. Detection gets all the love.* For the IC, prevention is not as stimulating nor as satisfying as detection. IC personnel see themselves more as Hunters than as Farmers.

The IC's strategy has been to do what the IC knows how to do best, not necessarily what is also needed to be done. Few in the IC know how to do anything besides detection. They believe they just need to be good Hunters.

HUNTERS AND FARMERS

Hunters and Farmers is one way to frame an understanding of how different brains work as understood within the psychiatric field of attention deficit disorder (ADD).

Hunters became a shorthand way of describing many with ADD whose style of coping depends on quick assessments, ability to shift focus rapidly, connect dots that others may miss, etc. In other words, even though ADD tends to be viewed in modern life as somewhat of a disability, these very same ADD traits during a hunt can be adaptive, useful and bring success.

By contrast, Farmers are slower, more detailed in their planning, must patiently deal with very long-term time horizons. Agriculture and the rise of civilization required these other types of minds.

I repurposed this dichotomy, Hunters vs. Farmers, used to better understand ADD, to help in rethinking insider threat management.

Familiarity with these novel conceptual simplifications, Hunters and Farmers, led me to reuse and adapt them for thinking about the different approaches that can be taken in the management of insider threat.

The IC does not know how to do fully effective prevention, which is more like Farming. The IC needs to cultivate Farming expertise too. Farming is what made mankind and civilization flourish, coaxing food out the ground using correct methods and timing, as dictated by nature. Hunting, always important, came to be recognized as having its limitations. Farming strengths began to surpass Hunter strengths.

"Farming" is the metaphor used here for gently coaxing employees "off the ledge" when they have moved beyond their capacities to cope with their disordered lives, so they will not go on to cross the line.

■ MEASURING SUCCESS: PREVENTION'S BIGGEST PROBLEM

Defining prevention success is hard. How do you know for sure if prevention efforts have worked when the measure of success is counting something bad that *did not* happen?

What do you count to prove success?

Einstein reputedly said: *"Not everything that counts can be counted and not everything that can be counted counts."*

Measuring success is hard when there is limited knowledge of a problem's baseline prevalence. All we know is how many insider spies have been caught. However, who believes that number represents a full accounting of the true number of insider spies? Optimistically, maybe there are only a few more out there than the number caught. Or, pessimistically, there may be multitudes still hidden away in the woodwork. The actual number remains a mystery.

■ PREVENTION RESOURCES TODAY NEED STRENGTHENING

The primary resources within each IC agency for prevention today are the employee assistance programs (EAPs) under their various IC agency names. Unfortunately, these EAP resources are not set up to manage the most serious cases, the very cases for which help is most needed to head off insider threat events. Let's consider the classes of possible EAP users:

The Three Classes of Troubled Employees

Class A

- Minor problem levels
- More stable individuals in minor crises who voluntarily seek counseling
- Existing EAPs can work with them

Class B

- Medium problem levels
- Behavioral indicators of distress visibly leak out, so managers pressure them to get counseling
- Troubled individuals are required to go to EAP
- Sometimes EAP can help with these cases

Class C

- Most serious problem levels
- Employees in serious trouble who can somehow conceal their distress. No one can see them sweat

- They are also the ones who can do the worst damage
- These are the employees who don't dare show up at EAPs! They are familiar with the EAPs' corridor reputation: If they go to an EAP, the next thing that will happen is a call from their friendly security officer
- Next on the agenda will be these bad consequences:
 - Loss of their clearance
 - Loss of their hopes for promotion
 - Loss of a portion of their income
 - Loss of their job

Stories Heard from the Corridor

Sometimes State Department diplomatic security agents do not dare reach for help. They correctly fear that their hopes for promotion will be taken off the table. If they are no longer allowed to carry their weapons, they know they will immediately lose 25% of their pay.

Some National Security Agency (NSA) managers have been known to explicitly warn subordinates *not* to seek help. They helpfully explain that it will become a nightmare for the troubled officers (true), but even worse, for themselves too.

Net Result:

Employees of greatest concern, with the most serious problems, are the very ones who will not dare make the call for help and will never show up at their home agency's EAP. How do you spell "disincentive?"

EAPs Today Are Like Urgent Care Centers

Urgent care centers, also known as "docs-in-the-box," have sprung up everywhere because in the medical world they satisfy a market need. They are cheaper, quicker, nearby, and handy, with locations everywhere.

Urgent care centers are very useful but are limited in what they can treat depending on severity of condition. They are geared up to deal with minor illnesses and some medium-level medical concerns. For medically dire situations, like severe trauma or life-threatening illnesses, there is no substitute for a full-fledged emergency room.

EAPs, like urgent care centers, are incapable of serving the most serious cases within the IC: Employees who are struggling with personal crises equivalent to major medical emergencies. That is because EAPs *are not perceived to be safe resources*. EAPs are there in the

org chart ("We've taken care of that"), but they do not provide help for the very cases for which they are most needed. EAPs are good for Class A and even Class B, but not Class C employees.

SUMMARIZING:

In the IC, we have urgent care centers, but no full-fledged emergency rooms necessary for the ones who need it most: Class C employees.

SECTION G

BUILDING A NEW COMPREHENSIVE PREVENTION PROGRAM

GENERAL CONSIDERATIONS

■ IMIT CONCEPTS WILL BE ITS GUIDING PRINCIPLES

Key Concern: Safety is Number One

Resources that are not perceived as safe are the same as no resources.

Anyone in big trouble today understandably fears seeking help because they worry it will only make things worse. They are concerned that communication between their home agency's EAP and their security and counterintelligence components is too direct, free, and easy.

Safe, government-sanctioned, confidential help would make all the difference. Only if such resources were seen as trustworthy and practical would employees consider it worthwhile to take the risk and give them a try.

"Lean on Me"

"Lean on Me" is a song that communicates a warm and caring invitation for accepting help, especially aimed at men whose pride tends to get in the way.¹⁴

Initial Contact: Making It Safe

For anyone overwhelmed by serious problems, it will be scary merely to explore the possibility of starting to seek help and counseling. Before getting started in earnest, there would have to be a delicate dance of exploratory contacts designed to be very secure.

Off-Ramp Exits Needed Before Someone Crosses the Line

Well-crafted off-ramp exit solutions will work if based on sound psychological principles. This requires in-depth understanding of the psychology of the target audience: Men undergoing the worst personal crises of their lives who feel like they are drowning.

Rapid

Interventions cannot be slow moving. Fast pacing is key. Interventions must immediately relieve the pressure so employees can quickly work their way out of their *Psychological Perfect Storms*. Think of helping a drowning person climb out of a raging river to the safety of the riverbank. Only once he feels safe will he be able to catch his breath and start to think clearly again.

Remove All Barriers

Barriers to entry need to be lowered to zero.

The price must be right: Free.

By removing any excuses to avoid reaching out for help, including financial, good things can start to happen. If there were no costs, there would be no excuses.

Comprehensive and Practical

EAP personnel will have to fix whatever needs fixing – and right away. Whatever it takes. Help must be provided across all areas of need, including financial.

EAPs must be delegated authority to effect or negotiate changes, including in the work setting:

- Leaves of absence
- Reduced work hours
- Change of work unit
- Change of supervisor
- Medical referral
- Marital counseling
- Help with children
- Anything else necessary

USEFUL STARTING FACT: ABOUT 90% OF INSIDER THREAT ACTORS ARE MALE

Males constitute about 90% of caught spies.

As a medical doctor, I am proud to announce that I discovered the genetic marker for insider spies: The Y chromosome.

This fact alone provides a valuable edge: the ability to sharply target messaging to the correct audience: to men, not so much to women. Therefore, understanding male psychology becomes key. Please read my *White Paper: Part One: True Psychology of the Insider Spy*, for a complete treatment of this subject.

INTERVENTION WINDOWS: WHEN OPEN AND WHEN CLOSED?

■ INTRODUCTION

For timing interventions, it is important to head off crossing the line in the “foothills” of the process, before it shoots up into the “mountains.” By then, the process will have advanced too far, and potential insider threat actors will have become too alienated and impervious to corrective messaging.

Training and education efforts that set the stage for effective prevention are best timed to occur before Stage 2, the Stress/Spiral Stage, while the target audience is still functional, rational and open to influence, well before the decision to spy gets made.

TEN LIFE STAGES OF THE INSIDER SPY

Stage One: The Sensitizing Stage (Everyone experiences adversity)

Stage Two: The Stress/Spiral Stage (Psychological Perfect Storm)

Stage Three: The Crisis/Climax/Resolution Stage (Epiphany of a Solution)

Stage Four: The Post-Recruitment Stage (Euphoria, Learning Tradecraft)

Stage Five: The Remorse / Morning-After Stage (“What was I thinking? What have I done?”)

Stage Six: The Active Spy Career Stage (Rationalizations, Constant Stress, Drudgery)

Stage Seven: The Dormancy Stage(s) (Fantasy of Escaping)

Stage Eight: The Pre-Arrest Stage (“Let’s get it over with!”)

Stage Nine: The Arrest and Post-Arrest Stage (Insolence, Belligerence but really Shame)

Stage Ten: The Brooding in Jail Stage (Sadder, Wiser, Philosophical)

■ **FIRST OPEN WINDOW:
STAGE 2 (STRESS/SPIRAL STAGE):
BEFORE SOMEONE CROSSES THE LINE**

The prelude to crossing the line consists of gradual shifts in the thinking of severely stressed and vulnerable individuals experiencing life pressures that pile up beyond their capacities to manage. This is an internal process, deliberately kept invisible to observers because of male pride – no one wants to let anyone else see them sweat.

If their thinking progresses to consider more extreme and desperate survival efforts, it starts to resemble falling into quicksand: the more they struggle, the more they sink even deeper, and the more they panic. That is when dangerous, irrational ideas of how to rescue themselves start to fill their minds – epiphanies of how to brilliantly solve every aspect of the terrible fixes they are in – by undertaking the drastic act of crossing the line.

■ **INTERVENING DURING EARLY
AND MID-STAGE 2**

Since it is still early in the progression, this is the ideal time to communicate corrective messages that offer well-packaged help. This is the last window of opportunity to do so before an employee finally decides to cross the line.

Once an employee progresses past some indefinable transition point, it is too late. The window closes. Their *personal psychological bubble* becomes impervious to rational guidance and restraint.

■ **CLOSED WINDOWS:
STAGES 3 AND 4: THE BLACKOUT PERIODS**

Windows are closed from just before to during and immediately after the decision to cross the line. During Stage 3 (Crisis, Climax, and Resolution Stage) and Stage 4 (Post-Recruitment Stage), the employee who is teetering on the edge of readiness to cross the line, or has just actually done so, is too flushed with excitement and misguided purpose. Temporarily, nothing can penetrate his agitated state, he is in a feverish, altered reality and can no longer exercise clear judgment. Thus, there is no power to intervene.

■ **OPEN WINDOWS:
STAGE 5 (REMORSE, MORNING AFTER STAGE);
STAGE 6 (ACTIVE SPY CAREER STAGE); AND
STAGE 7 (DORMANCY STAGE):
THE STAGES AFTER SOMEONE CROSSES THE
LINE**

The heat of the moment will subside some months after having crossed the line, at which point the insider spy may realize he has made a terrible mistake. He recognizes he is stuck, trapped, and helpless, with no way out. These are the stages where an off-ramp exit option, the proposed NOIR mechanism, can offer a pathway out, which will stop the hemorrhage of our national security secrets.

See my *NOIR White Paper: Part Two* for a detailed explanation of these off-ramp options.

TWO-TIER STRUCTURE ADVOCATED FOR EAPS

■ **FIRST TIER: EXISTING EAPS INTERNAL
TO EACH IC AGENCY**

Main improvements needed to shore up existing internal EAPs include:

- More robust outreach to employees made with communications that align with the recommendations that are described below
- Firewalling of agency EAPs from management, security, and CI components

Advantages

Internal EAP personnel know their own agency culture intimately and have relationships with other home agency personnel, including management at all echelons. They are logistically handy since they are located on the premises.

Disadvantages

Internal EAPs tend not be trusted if there is a history of too much direct, free and easy communication with their home agency's security and CI components. Employees may be concerned about showing up on the premises of their internal EAP and run into people they know: "Jim, what are you doing here?"

After initial crisis management, employees may have to be turned over to another counselor for more long-term help. They may have to engage with a new person they may not like. They may need to tell their whole story all over again.

■ SECOND TIER: A SECOND-LEVEL EAP — EXTERNAL TO THE HOME AGENCY

This option could be thought of as an EAP “at a higher level.” Standing up this new resource is essential because negative corridor reputations are hard to overcome. If an employee has a significant problem with their home agency, they will not expect to be treated fairly by its EAP. *They just will not go there.* If employees do not trust their home agency’s EAP, they absolutely need an external EAP!

Advantages

An External EAP may be perceived as more trustworthy and safer regarding confidentiality simply because it is not attached to their home agency.

Disadvantages

External EAPs are less convenient since they are located further away.

External EAPs may not understand the inner workings of the home agency as well as internal EAPs.

RESOURCES MUST BE REAL

To truly fulfill promises to help, the IC cannot make promises that are not kept.

Resources offered need to go beyond psychological counseling.

They must also provide the following kinds of counseling:

- Financial, including easy loans
- Legal
- Tax and accounting
- Career counseling
- Guidance addressing any major life stresses

■ AN EXTERNAL EAP HAS THE ADVANTAGES OF A THIRD PARTY

As a third party, an external EAP provides a safer outlet since it is a step removed from the home agency. That distance makes it easier to vent and burn off intense negative feelings that troubled employees may harbor towards their distrusted home agency. A neutral third party can absorb hostile emotions based on bad experiences with antagonists within the employee’s home agency, thus acting as a pressure release valve. As a government-sanctioned IC resource, the external EAP would be seen as safe since cleared counselors would staff it.

The external EAP’s role would emulate private sector outplacement firms. Their job is to solve employee problems, and if necessary, ease them out — *but gently, gracefully and respectfully.* The aim is for “soft landings,” which benefits the employee and the company.

■ RESOURCES

What is Needed and Why

Resources should be aimed at relieving the desperate employee’s feeling of drowning *as soon as possible*, doing whatever it takes, whether problems are financial, relationship or work-based. A quick and immediate fix is critical. Afterward, there must be follow up with more careful long-term intervention for further repair and healing.

Cost considerations must be made subordinate to the larger goal of prevention. All it takes is one Hanssen or Snowden to underscore that the cost tradeoffs are clear: How many billions of dollars did it take to repair the damages of just these two insiders?



How many billions of dollars did it take to repair the damages of just these two insiders?

to repair the damages of just these two insiders?

More on costs: It is important for the IC to keep its eye on the ball. To illustrate this critical point, imagine a genie who says: “I’m willing to turn the clock back to just before Snowden (or Hanssen, etc.) gave away all your precious secrets. You won’t have lost any of them! How much would you be willing to pay?”

Setting Up Resources Will Not Be Simple

Staffing Personnel Will Be Challenging

Recruiting, vetting and selecting counseling staff who meet demanding criteria:

- Experienced in the counseling field
- Familiar with the IC
- Understand the mission
- Engaging, warm, and personable

- Non-judgmental
- Practical
- Possesses skills to extend crisis counseling into longer-term follow-up

Specialized Training Will Be Needed

To handle “hot potato” cases, relieving the pressure rapidly.

Authorities

Staff will need to be given authority to make decisions and initiate actions that get the job done at whatever the cost – because the costs of failure to contain problem employees are likely to be vastly more than the costs of not heading off the threats. “Pennywise and pound-foolish” in these matters makes no sense.

Primary Aim: Rescue a basically good employee and get him back to work.

Separation from service must remain an option

Separation, in some cases, will be the better choice. Some employees will not be rescuable. Exercising this option would have to be carefully orchestrated to achieve the desired “soft landing.” The proposed NOIR mechanism would be best for managing this outcome. For this reason, there is a rationale to simultaneously stand up both the proposed prevention resources, as well as NOIR, because the combination of both would create a seamless suite of off-ramp exit solutions, for the situations *before* and *after* crossing the line.

Case Manager Approach

Case managers can be the good (traffic) cops, advocates for the best interests of beleaguered employees. Though they are not psychological counselors, case managers can orchestrate setting up a variety of counseling resources and can communicate and coordinate with all relevant parties.

A case manager approach makes the process of getting help more human as compared to being handled by a cold bureaucratic machine. Employees will think: “At least there’s one good, decent person I can trust who will watch over my progress from start to finish.”

Case managers can carefully communicate with the home agency and its internal components, such as security and CI. Initial contact with the case manager must be made simple, clear, and easy.

Security Concerns

Concealing the identities of counselors and employees from certain interested parties who have potential to cause trouble will be important. That includes our own security investigators who will initially need to be kept at arm’s length. Otherwise, employees will get spooked, which will wreck their trust in the process. Sticking to such careful guidelines will preserve the new prevention program’s good corridor reputation. Losing a good corridor reputation risks wrecking the whole program.

FIE agents would also be threats. They would love to know who is in severe distress because, of course, these are the employees who would be their best targets to recruit.

MAKING THE NEW PREVENTION PROGRAM WORK

■ TARGETING THE CORRECT AUDIENCE

Who are the correct targets? To make the new prevention program work, it is essential to know with whom you are dealing. Potential insider threat actors are described in my *White Paper, Part One: True Psychology of the Insider Spy*.

Potential insider threat actors are feeling desperate. They process their overwhelming life situations from distorted perspectives, mirroring the mindsets of patients with clinical anxiety and depression. They are not thinking like their usual selves. They are operating with skewed logic and a dark worldview, pessimistic and hopeless. Their sense of time has collapsed into a constant terrible Now, with no memory of a better past or any anticipation of a better future. Their extreme emotional states may include:

- Depression
- Demoralization
- Broken pride
- Feeling like a failure
- Desperation
- Agitation
- Scared
- Panicked
- Struggling
- Drowning
- Exhausted

THE EXAMPLE OF EARL PITTS

Earl Pitts, the first insider spy I worked with, pointed out parallels to his own mental state before he crossed the line described in a *Newsweek* article published after US Navy chief of naval operations (CNO), Admiral Michael Boorda's suicide.*

The article discusses "executive suicides," describing unexpected, incomprehensible suicides by high-level executives at the tops of their games.

These executives apparently experienced tremendous internal pressures trying to make sense of their high outward achievements that did not match up with their own extremely critical self-appraisals.

When they felt threatened that their charades were disintegrating, they saw no way out other than suicide.

*Newsweek Staff, "A Lonely Death in Texas," *Newsweek*, 30 March 1997: www.newsweek.com/lonely-death-texas-170434.

- Poor judgment
- Inability to focus
- Angry and aggressive in all directions

After the crisis passes, they will not believe they were temporarily so totally captured by such twisted emotions and logic. As they get restored back to their usual competent selves, they will dramatically shift to more positive perspectives.

■ COMMUNICATING THE RIGHT WAY WITH THE TARGET AUDIENCE

Adopt the Proper Tone

Speak to their desperation, inner hurt, and pain; not to their outward prickly defenses. See the lessons from the previous discussion of handling hostage takers.

Engage by Making Offers Instead of Threats:

- Lifelines with reassurances
- Quick, immediate help
- Respectful tones that preserve pride
- No threats

- Safe
- Framed as the *manly* thing to do
- Emphasize *hope*

Off-ramp exit options would be proposed as the employee's choice to make, freely, voluntarily, and only when ready. Offering choices is always preferable. Even children prefer choices. Choices work better than forcing demands, which just raises resistance. Remember the old saying: "You can catch more flies with honey than with vinegar."

■ PACKAGING OFFERS

Offers must be sensible and attractive. Offers must address prospects in respectful terms, packaged in ways that will restore the employee's sensitive bruised ego. Offers must preserve the employee's pride and dignity. There would be no room for authoritarian, scolding, threatening, or coercive messages. Done this way, offers restore hope to an employee on the ropes, overwhelmed and impaired by compromised thinking and logic.

NEW PREVENTION PROGRAM SHOULD BE ROLLED OUT IN PHASES

■ PHASE ONE: REDEFINING THE MEANING OF SPYING

Redefining the meaning of spying would be a critical first step that sets the stage for changing basic assumptions about spies and insider threat actors.

For example, current basic assumptions and theories about insider spies are that they are simply bad people, criminals, evil schemers, and traitors to their bones. Certain personality characteristics have been attributed to insider spies who were studied, such as *narcissistic*, *grandiose*, *antisocial*, etc.¹⁵ When examined more closely, these diagnostic terms can be better understood as *defensive* in nature. They serve to cover up to the world, and more so, to themselves, the deeper core problem of insider spies: *An intolerable sense of personal failure, as privately defined by that person.*

These negative characterizations, while not wrong, are superficial. They do not help much in identifying potential or active insider threat actors since they are found so frequently in all populations, especially in high-performance, driven professionals. They are not precise enough to warrant investigating the many employees who are wired this way. Can you picture saying to an employee: "We think you are arrogant, so we have to take away your clearance."

These pejorative terms, though they sound diagnostically significant, do not amount to much more than after-the-fact name-calling. To discern the core psychology from which these tendencies originate, delving deeper is important. Going beyond characterizing spies as just being evil criminals is necessary.

Paradoxically, in our country, being bad can be an attractive identity and pose. Spies may be oddly proud of being BAD. Working to change the real meaning of spying from being BAD to being SAD becomes a useful goal.

Simply put, spies are unhappy people who have failed in their lives.

They are not so much evil, malicious criminals as hurt, injured, fragile, failing people. They see themselves as Losers and Failures. The *redefined meaning of spying* is solidly based on key NOIR White Paper ideas. These ideas should be referenced because they go a long way towards explaining what is behind the drastically bad decision to cross the line.

More on Redefining What Spying Really Means

Crossing the line is no longer to be defined as just being a criminal, vengeful, evil act of a defiant outlaw (although it is all these things). Because there is a dark attraction in our country to being labeled in these negative terms, why go along with something that just adds gasoline to the fire? There is truth to the old saying: "People would rather be hated than ignored." Ignored in this case means being regarded as small and insignificant, intolerable for any man's sense of pride.

The decision to spy must be transformed in the minds of the general public, and especially within the minds of the IC workforce, into something rather different:

Crossing the line is more a desperate and profoundly sad act that reveals evidence of a fellow human being's ultimate failure. It reveals that a broken coworker became a pathetic human train wreck, whose last-ditch effort to feel better about himself was to cross the line.

Can a Commonly Held Assumptions Be Changed? Yes, If Done Right

CASE EXAMPLE:

Trashed Texas Highways Get Cleaned Up

When citizens of Texas had enough of their littered and trashed highways, they brainstormed ways to get them cleaned up. They created a program with the

catchy slogan: "Don't mess with Texas."¹⁶

This slogan appealed not only to famous Texas pride but also to individual masculine pride and ego. No Texas dude ever wants to be

messed with. That would be an intolerable insult. With the new catchy slogan, individual male attitudes about pride were extended and attached to the entire sovereign state of Texas. Now, not trashing Texas highways became not just a matter of individual pride but also of collective pride, joining something that always had personal meaning to a *larger purpose*. Messing up Texas highways was now conflated with messing with each and every Texan's personal reputation. Don't ever think about getting away with that!

To disseminate the new message took a concerted program costing time, energy and money. But when the desired attitude took hold, Texas highways got clean.

Redefining the real meaning of spying within the general population and the IC workforce will take about two years of concerted effort.

How Redefining the Meaning of Spying Helps Change Inner Calculations

Redefining the meaning of crossing the line, from *bad* to *sad*, builds a self-limiting mental barrier that will work internally on prospective spies, forcing them to reconsider their impending rash decisions. For the sake of their residual pride, they will redouble their efforts to work out different, saner solutions.

Implanting the new meaning of insider spying inside the minds of employees on the brink to "Not so much bad as sad," will build *internal resistance* to allowing any further slide down the slippery slope. What remains of their personal pride will now come to the rescue: "I'm not a loser/failure. I *can* find another way to beat this!"

Any employee contemplating crossing the line will be preconditioned to know what crossing the line will mean, not just to themselves, but to everyone else: That they have *utterly failed as a person*, a shameful reputation to have to live with.



They will have to anticipate that, if they do cross the line and do get caught, the public will eventually hear their story of betrayal. The public will share an instant understanding of what it really means. Instead of caught spies being on the receiving end of mere anger, they will be on the receiving end of *pity*.

No one wants to feel pitied.

The redefinition, from *bad* to *sad*, will be coupled with the companion message that when you know you need help, it is the manly thing to reach for it.

Again, the words of the song “*Lean on Me*”¹⁴ capture the right tone to be communicated.

■ PHASE TWO: PROVING THE REDEFINED MEANING OF SPYING

You cannot make a big claim without providing proof. Fortunately, the proof is not hard to come by to support the narrative that in the months before deciding to cross the line, most potential insider spies have

suffered a severe and *sad* downward spiral in their lives. You do not have to make up the stories. The tragic stories of caught insider spies showing this linkage are already very well known. The stories give support and life to the proposed redefinition.

These sad stories just need to be gathered together and presented

as examples proving the point, making the case that a fellow human being, under extreme stress conditions, broke under pressure. When unhappy people lose control of their lives and lose their self-respect is when they start their downward slides, the precise state of mind that makes them candidates for crossing the line and perpetrating insider threat events.

There is nothing here to admire. Rather, it is a sad and depressing story when overwhelming life pressures destroy a good intelligence officer.

Spying will get recast as *equivalent to the worst personal humiliations*. Spying would get redefined as the adult equivalent of the worst humiliation that can occur to a kindergarten kid: Making in your pants. There is no honor or anything good to say about it. It is embarrassing, all too obvious (it stinks), and worst of all, shows everyone else that you are still just a baby!

Does it matter that this redefinition fully explains every single case? No.

Consider the Power of Memes

Memes are ideas or notions that propagate through populations somewhat like biological genes, though mainly by word of mouth, or these days, through social media. If an idea or meme sticks, it develops a life of its own and spreads virally. If most people come to believe the explanation makes sense, it will become the shared, accepted truth.

The mere repetition of memes makes them gain acceptance if there are enough supporting proofs to back them up. Given enough time, the redefined meaning of spying will change to:

Some unfortunate coworker couldn't handle his life stresses and got broken by the pressure. That is why he crossed the line.

Spying is the ultimate proof that he was destroyed, reduced to be a complete loser, a total failure.

What a pity he broke. How sad and disappointing.

■ PHASE THREE: GETTING THE MESSAGES OUT

Messages must be proactively publicized and implanted into the minds of the general public and the IC workforce by using techniques from the worlds of marketing, advertising, and promotion. No need here to describe the advanced

publicity methods practiced in our country for decades.

Focus groups could come up with the best language, words, and phrases to use for capturing attention and being well received. Messages must be coupled with appeals to residual pride and ego.

For example: “If you really put your mind to it, you can find other ways to solve your worst life crisis. Better ways. More mature and adult ways. You can dig your way out of your hole. Don't dig the hole any deeper!”



Outreach to the General Public

Limiting this campaign to just the IC workforce is not enough by itself. The redefinition must be shared throughout the entire culture of our nation to achieve the beneficial effect of changing internal calculations about what it means to cross the line. Everyone on the edge of crossing the line will have to calculate how their decision will later play inside the minds of fellow employees, friends, family, and the general public.

NEW SECURITY TRAINING FOR THE IC WORKFORCE

Semi-Annual Computerized Training

The *Core Psychology of the Insider Spy* and the *Ten Life Stages of the Insider Spy* should be taught, as well as the redefinition of what spying (or becoming an insider threat actor) really means, as described above.

The redefined meaning of spying must be proven with true sad life stories as evidence. Themes to be explored will include: What were the life pressures that set up troubled employees to get into their difficulties, what were the backgrounds that sensitized them, how and why did they break under the pressure? There would be dramatized portrayals of typical crisis situations that are paired with portrayals of alternative scenarios showing how to better handle similar life stresses.

New helping resources will be described

The first message to be conveyed is that things are different from the way they used to be. In the past, helping resources may have been regarded as not so safe or trustworthy, maybe even too dangerous to try. Employees used to avoid seeking help for fear it could make things even worse. But the situation is better now. IC leadership came to understand the deficiencies and took decisive steps to remedy them. There is now a new prevention program in place, which includes an external EAP, outside every employee's home agency, for those who will feel safer and more comfortable with such a resource.

Examples of life situations that can be helped would be listed. Workarounds would be described as well as the range of resources that are now available.

EXAMPLES OF NEW MESSAGING:

"Your country still needs you."

"You're still valuable."

"We will help you, whatever it takes. It makes sense for you; and for our national security."

"We have two tiers of help available. You can decide which one will work better for you: Your home agency's EAP or our EAP outside your home agency."

"Our EAP outside your home agency may make you feel safer if you have a serious beef with your home agency. We can help. We're at a higher level."

"Overwhelmed right now? Happens to the best of us."

"Things can pile up. Feel painted into a corner? Can happen to anyone. Want some brilliant advice? Stop painting!"

"Real courage defined: Guy gets cornered, but still figures out smart, honorable ways to get himself out of that corner."

"Think about all the stories you've heard, the sad life stories of those who crossed the line. It seems like only losers cross the line. We think you're better than that."

"Get help when you know you need it. We'll make it safe."

"We still think you're a valuable person even if right now you may not believe it yourself. We still need you to contribute to the mission. Let's get you squared away and back into the game."

"Worried about telling our counselors about the fix you're in? Give a listen to the words of the song 'Lean on Me.'¹⁴

"Reach for help and exit the highway to nowhere. We put a lot into building a safe and honorable off-ramp exit for you. How about taking it?"

"Take your life back!"

The new two-tier structure of EAPs would be explained

- The First Tier: Home agency internal EAPs
- The Second Tier: The external EAP

Resources for *after* crossing the line, such as NOIR (should it be stood up), would also be described.

Live Events

- Presentations, lectures, movies
- Panels of actual spies who were caught

Insider spies, whether still incarcerated or now released, would tell their stories in their own words. This event would have powerful impact since the people telling their stories would be former IC employees. Their stories would be told candidly, pulling no punches, recounting their unhappy experiences with the sadder-but-wiser lessons they learned. This would resemble panels of impaired MDs who have told their stories to fellow physicians, an enormously powerful experience for such audiences.

MESSAGING

Messaging must be to the entire IC workforce

Of course, that is mostly preaching to the choir because nearly the entire IC workforce is solidly loyal, patriotic and would never think of crossing the line.

True targets are those who are currently severely stressed and vulnerable

It is especially necessary to speak to them. If they are not moved by this outreach, there is no chance of effective prevention. Messaging must reach those who are “on the ledge,” already deeply mired in desperate situations. Words, phrases, and language must be used that can still reach and move them. Messages must offer empathy and rays of hope, and resources that are safe, make sense, and that would be regarded as credible rescue options.

Messages must go under the radar by communicating caring concern

The tone of messaging can no longer be the usual messages consisting of dire warnings not to cross the line, that threaten severe punishments, or that admonish with negative, scolding tones. Messages communicated in a “military voice” will be reacted to with anger or will just be ignored.

Messages must go under their defensive radar and speak to their underlying *intolerable sense of personal failure*. The revised tones must communicate concern and sorrow for coworkers and teammates who are no longer able to manage their lives and who are feeling overwhelmed, desperate, cornered, drowning.

The new tones would show that the IC understands that they are feeling desperate, hopeless, exhausted and out of ideas of how to steer their lives and survive.

By accurately identifying how they are feeling and communicating that understanding in language and words that penetrate through their mental fog and confusion, the new caring and persuasive messages will not get deflected so easily and will penetrate false defensives. Employees “on the ledge” will be thrown off balance *in a good way* by these caring messages. They will be forced to face themselves without the protection of their chosen armor.

Given the psychological truth of what is going on, aren't these new messages more on target and appealing?

If a sailor falls overboard, you don't lecture him from the rail about why he should have taken more swimming lessons. You throw him a lifeline!

Not: “We watch everything you do and if you cross the line, we'll catch you, you slime!”

LOCATE SECOND-TIER PREVENTION RESOURCES UNDER THE ODNI

Despite initial misgivings about the Office of the Director of National Intelligence (ODNI), its mission has been to make the entire IC work more effectively. Located within the ODNI, the external to the home agency EAP prevention function would provide a valuable resource that could be made available across all sixteen IC agencies. As explained, it is important for the perception of safety to have an external, second-tier resource that operates outside of the other sixteen IC agencies, thus able to act as a third party with its many advantages.

■ BEST PRACTICES

For the sake of improving the prevention function, refining it would be better accomplished within one central, expert setting. Otherwise, best practice refinements may get lost inside the stovepipes of the sixteen separate IC agencies. Learning how to set up helping resources will be based on best practices borrowed from existing successful counseling systems, combined with IC tradecraft knowledge.

ODNI-located resources can house the two key capabilities that should *not* be housed in the individual agencies:

- The second-tier external EAP, the EAP “at a higher level”
- NOIR

Detection must still be conducted by security and CI within each IC agency

Detection is still a critical function that must be performed by each agency’s security and CI components. They are familiar with the details and culture of their respective agencies.

Could someone abuse the proposed prevention system? Not to worry.

What about concern that some scheming employees might abuse and exploit the new prevention system? Maybe they just want to escape their job and take the easy way out?

Please don’t throw me into that briar patch!

This should not be regarded as abuse. This should be thought of as a gift from God.

If someone reaches out to the second-tier level of help as their plan to “abuse” or “exploit” the system, so what? Aren’t these the very employees that you would desperately want to be removed from access to classified materials? If they want out that badly, don’t you also want them out even more? Isn’t that far better than the alternative: a sudden deluge of classified materials released to our adversaries or to the public?

The price to exit such types will be tiny compared to the cost of the damages they might otherwise inflict. Whatever the costs, it is still cheaper to handle it this way. Remember the genie question posed earlier. There is no point being “penny wise, pound-foolish.”

Some may be genuinely difficult people

Still, a soft-glove approach should be employed. It is important for the IC to keep eyes on the prize: What is it that nets out best for the IC? What meets the crucial goal of more successfully preventing insider threat events?

■ EMPLOYEES TEMPORARILY IMMUNE TO PREVENTION MESSAGES

Whistleblowers

Early in the game, they may see themselves as strictly motivated by high-minded, “noble” intentions. Their rationalizations are still too attractive to them. That can change.

THE BRIAR PATCH

The “briar patch” noted above harkens back to the proverbial stories of Uncle Remus, an African-American version of Aesop’s Fables, compiled by Joel Chandler Harris, that illustrate human nature and foibles.

Brer Fox captures Brer Rabbit. This could be the end for Brer Rabbit, but Brer Rabbit starts moaning, groaning, and crying. He begs Brer Fox to do anything he wants, tear him limb from limb, but “*please, please, don’t throw me into that briar patch!*”

Brer Fox cannot help but decide that if throwing Brer Rabbit into the briar patch would inflict the very worst on that rabbit, that’s exactly what he will do! Of course, Brer Rabbit is steps ahead of Brer Fox. He knows the briar patch is impossible for the fox to navigate, whereas as a rabbit, he can get along fine inside the briars, and will be able to escape to live another day.

No one in the IC would want to have a risky person “get away” with the easy outs proposed by the off-ramp exits I have proposed. But that misses the IC’s highest goal regarding insider threat: Stop it cold, get them out if necessary, and do so at whatever cost! It is infinitely cheaper to manage potential enormous losses of classified information that way as compared to all the alternatives.

Employees with ethnic, ideological, or religious motives

In the early stages of their recruitment, clever appeals and arguments invoking such tribal loyalties may still be too convincing to them. Initial compelling motivations can change over time since such rationales often weaken over time.

Psychopathic and antisocial types

These personality types are unlikely to be moved by appeals to seek help. However, all is not lost. For strictly selfish reasons, when they calculate it is advantageous for them, they may decide to reach for help anyhow. Is that a problem? Why? They would have to *voluntarily self-identify* and now become visible. This alone will cause them to have to cease their harmful activities. The IC would still be in better shape because now, having even

partial knowledge of their identities, the situation would be much better than having no knowledge of them. This affords the IC a great advantage compared to merely hoping that someday, perhaps many years from now, detection will luck out and disclose them.

Not yet ready

Employees who are just not yet ready because they are still too preoccupied with their internal mental struggles to consider alternatives. Exit options will have to wait a while longer until changing life circumstances will increase their readiness.

NO CLAIM THIS NEW PREVENTION PROGRAM IS A PERFECT SOLUTION

Imperfect is good enough. As they say: “The perfect is the enemy of the good.” No program will ever be perfect and work for all insider threat actors. Less than perfect outcomes are predictable, but that is better than a multitude of really terrible outcomes. The proposed new prevention program is guided by the notion: *Problems can be solved, messes must be managed.*

The primary goal is to significantly reduce the prevalence of insider threat events.

NOIR can be the backstop for those who were not persuaded by the new prevention program and still choose to cross the line. NOIR is for those who later experience an awakening and voluntarily decide to quit their treasonous activities. If the new prevention program advocated here does not capture insider threat actors *before* they choose to cross the line, there is still the chance to capture them *after* they have crossed the line – but only if NOIR also gets stood up as the companion back-end resource.

LEGAL HURDLES TO BE OVERCOME

Do these three NOIR white papers with their proposed novel and controversial mechanisms assume there will be no conflicts with our existing system of laws related to insider threat and spying?

While I am not an attorney, it does not mean I am completely naïve. Adoption of the NOIR proposals would surely encounter serious conflicts with existing laws, procedures and practices. That is why buy-in from all agencies of the IC, especially the Department of Justice (DOJ), would be necessary. Acceptance by Congress, the White House and the general public would also be necessary. A very hard sell.

That said, roughly the same set of barriers and hurdles existed when the Witness Protection Program (WITSEC) was first proposed decades ago. For WITSEC to gain acceptance from the interested



parties mentioned above was initially seen as virtually impossible. Fortunately, WITSEC was backed strongly by then Attorney General, Robert Kennedy, and of course, by his brother, President John F. Kennedy. Both were determined to bring down the American Mafia. They decided this could only be accomplished by creating a safe exit mechanism for Mafia gangsters, who could then tell their incriminating tales, though still at real risk to their lives. It worked.

Hard decisions were made at the highest levels to subordinate national revulsion at giving a pass to criminals and murderers in exchange for the strategic advantage of ridding our country of an even greater evil, the Mafia. Gerald Shur of the DOJ was the hero attorney who guided WITSEC through all the legal barriers, at some personal risk of his own. WITSEC continues to operate effectively today, managed by the United States Marshals Service.

As with WITSEC, overcoming the legal hurdles that will permit NOIR proposals to successfully get adopted will take a lot of hard work. Similarly, it will be worth it.

NOIR concepts were partly inspired by and echo the story of WITSEC, adjusted for utility within the IC. Critical benefits of admittedly controversial programs sometimes can be sufficiently advantageous to justify the difficult accommodations that would be required to give them life. Especially so when the stakes are so important – our national survival. With the aim of much improved management of insider threat, there is a rationale to change existing laws when the stakes are existential. Quoting Justice Robert H. Jackson: “The Constitution is not a suicide pact.”¹⁷

SECTION H

CONCLUSIONS

DETECTION IS NECESSARY BUT NOT SUFFICIENT

Within the IC, most thinking and resources have gone into detection even though exclusive reliance on detection has not proven to work that well. Of course, detection is clearly absolutely necessary and works up to a point. Unfortunately, when a determined insider decides to defeat detection measures, they succeed all too frequently. Relying exclusively on detection is insufficient. We need more tools in our toolkit.

MISSING LINKS: TWO OFF-RAMP EXITS

Two important links are missing for creating a *full spectrum solution* for better management of insider threat: Off-ramp exits for *before* and off-ramp exits for *after* someone crosses the line.

TO MOVE “LEFT OF BOOM,” A FULL SPECTRUM SOLUTION IS NEEDED

Solutions to be added are based on a better understanding of the psychology of insider threat actors. The three most important strategies that are advocated in this paper:

1. **Elevating IMIT approaches to managing insider threat**, as opposed to almost exclusive reliance on EMIT approaches
2. **Redefining the meaning of spying** to build self-imposed inner resistance in the minds of troubled employees, to help prevent any further inclination to cross the line. Residual pride will come to the rescue.
3. **Improving existing EAPs and adding novel EAP resources** will provide exit solutions that are safer for troubled employees to access. These enhanced helping resources will work to restore what troubled employees are sorely lacking: *Hope*.

COMBINING FRONT AND BACK-END SOLUTIONS

Building off-ramp exit solutions for before and for after someone crosses the line would add the two most glaring missing links that are necessary to establish a *full spectrum solution* for effectively managing insider threat.

If it is not possible to head off insider threat actors *before* they cross the line, then the next best thing is to stop them *after* they cross the line, and the sooner, the better (NOIR). Simultaneously standing up both proposed off-ramp exit solutions would be more efficient, effective and practical.

FINAL MESSAGE

- We all share a common goal – protect our nation’s security from insider spies and insider threats
- We have a number of tools in our tool kit: prevention, detection, deterrence through prosecution, etc.
- We have challenges and opportunities in all of these areas
- None of these tools, alone or in combination, is a silver bullet
- Detection using big data analytics, ML and AI may become revolutionary but are not problem-free
- NOIR proposals add more tools to our toolkit: exit ramps for before or after someone crosses the line
- Adding the new resources proposed in my three NOIR papers is not a choice to be made in opposition to detection – they are complementary to detection

Will the IC take up the challenge of managing its insider threat risk by going beyond mainly relying on detection? Will the IC strengthen its insider threat posture by adopting the new prevention strategies proposed in this paper?

There is hope. Churchill supposedly said: “Americans can always be counted to do the right thing... after they’ve tried all the other possibilities.”

ENDNOTES

¹ Sun Tzu, James Trapp (trans.), “Chapter VII: Maneuvers Against the Enemy” in *The Art of War*, (New York: Chartwell Books, 2016): 47.

² *NOIR White Papers*: The first paper, entitled “True Psychology of the Insider Spy,” was first published in the *The Intelligencer* 18 (1) Fall/Winter 2010 47-54. *The Intelligencer* is the official journal of the Association of Former Intelligence Officers (AFIO). The paper was republished as a special attachment to *The Intelligencer*, as Part One of a two-part White Paper, entitled “NOIR, A White Paper.” Part Two was entitled, “Proposing a New Policy For Improving National Security By Fixing the Problem of Insider Spies.” To access all three NOIR White Papers, which are available online as PDFs, please refer to our website: NOIR4USA.org.

³ Martin Handford. First published in London as *Where’s Wally?* (London: Walker Books, 1987). There have been numerous follow-on volumes.

⁴ German Democratic Republic (GDR) Ministry for State Security (*Ministerium für Staatssicherheit*, MfS, Stasi) was the East German state security service, with both internal and external functions. In its internal functions, it is a classic example of a secret police force controlling a national population.

⁵ See details of the Behavioral Stairway Model at the Viaconflict Website, 26 October 2014: <https://viaconflict.wordpress.com/2014/10/26/the-behavioral-change-stairway-model/>

⁶ An excellent and thorough treatment of the development of these softer and more effective interrogation methods can be found in “The long read: The scientists persuading terrorists to spill their secrets,” London *Guardian*, October 13, 2017: <https://www.theguardian.com/news/2017/oct/13/the-scientists-persuading-terrorists-to-spill-their-secrets>.

⁷ As an example of the mounting concern, consider the following title of an industry publication with the wake-up call: “In 2017, The Insider Threat Epidemic Begins” by James Scott and Drew Spaniel (February 2017). <http://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf>.

⁸ Mike Rogers, former chairman of the House Special Select Committee on Intelligence, is quoted to this effect

in Julien Hattem, “Former Intelligence chairman: More spies than ever,” *The Hill*, 30 March 2016: <http://thehill.com/policy/national-security/274704-former-intel-chairman-more-foreign-spies-in-us-than-ever-before>.

⁹ John R. Schindler addresses this issue in “Our National Security’s Millennial Problem,” *The Observer*, 14 October 2017: <http://observer.com/2017/10/snowden-winner-manning-nsa-millennial-problem/>.

¹⁰ Alden Munson wrote a biting account of his experiences in “Why Can’t We Get Acquisitions Right?” in *STEPS: Science, Technology, and Engineering Policy Studies*, October 2017. He describes the forces that work against sanity in how government sets about acquiring new systems as “the Conspiracy of Hope.” <http://www.potomacinstitute.org/featured-news/1800-why-can-t-we-get-acquisitions-right-by-alden-munson>

¹¹ Will Knight, “The Dark Secret at the Heart of AI,” *MIT Technology Review*, 11 April 2017: <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/>

¹² Will Knight, “Biased Algorithms Are Everywhere, and No One Seems to Care,” *MIT Technology Review*, 12 July 2017: <https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/>.

¹³ Judge Webster addressed this concern in private conversation with me.

¹⁴ *Lean on Me* is a 1972 song that says it all. For a great performance, listen to the rendition recorded in 2009 by the country group Nothin’ Fancy. See: <https://www.youtube.com/watch?v=ZKzT1yrrlDc>. Also see song lyrics below.

¹⁵ These psychological and psychiatric terms show up in the IC’s most ambitious attempts at studying insider threat: the 1990 Project *Slammer* and the Defense Department Defense Personnel and Security Research Center (PERSEREC) studies.

¹⁶ “Don’t mess with Texas” website, www.dontmesswithtexas.org.

¹⁷ https://en.wikipedia.org/wiki/The_Constitution_is_not_a_suicide_pact.

Lean on Me

Written by Bill Withers • Copyright © Universal Music Publishing Group

Sometimes in our lives we all have pain
We all have sorrow
But if we are wise
We know that there's always tomorrow

Lean on me, when you're not strong
And I'll be your friend
I'll help you carry on
For it won't be long
'Til I'm gonna need
Somebody to lean on

Please swallow your pride
If I have faith you need to borrow
For no one can fill those of your needs
That you won't let show

You just call on me brother, when you need a hand
We all need somebody to lean on
I just might have a problem that you'll understand
We all need somebody to lean on

Lean on me, when you're not strong
And I'll be your friend
I'll help you carry on
For it won't be long
'Til I'm gonna need
Somebody to lean on

You just call on me brother, when you need a hand
We all need somebody to lean on
I just might have a problem that you'll understand
We all need somebody to lean on

If there is a load you have to bear
That you can't carry
I'm right up the road
I'll share your load

If you just call me (call me)
If you need a friend (call me) call me uh huh(call me)
if you need a friend (call me)
If you ever need a friend (call me)
Call me (call me) call me (call me) call me
(Call me) call me (call me) if you need a friend
(Call me) call me (call me) call me (call me) call me
(call me) call me (call me)

WWW.NOIR4USA.ORG



NOIR

PROPOSING A NATIONAL OFFICE
FOR INTELLIGENCE RECONCILIATION

FOR MORE INFORMATION, GO TO:

WWW.NOIR4USA.ORG