

mercury

INSIDER TRUST

PAUL FITZPATRICK

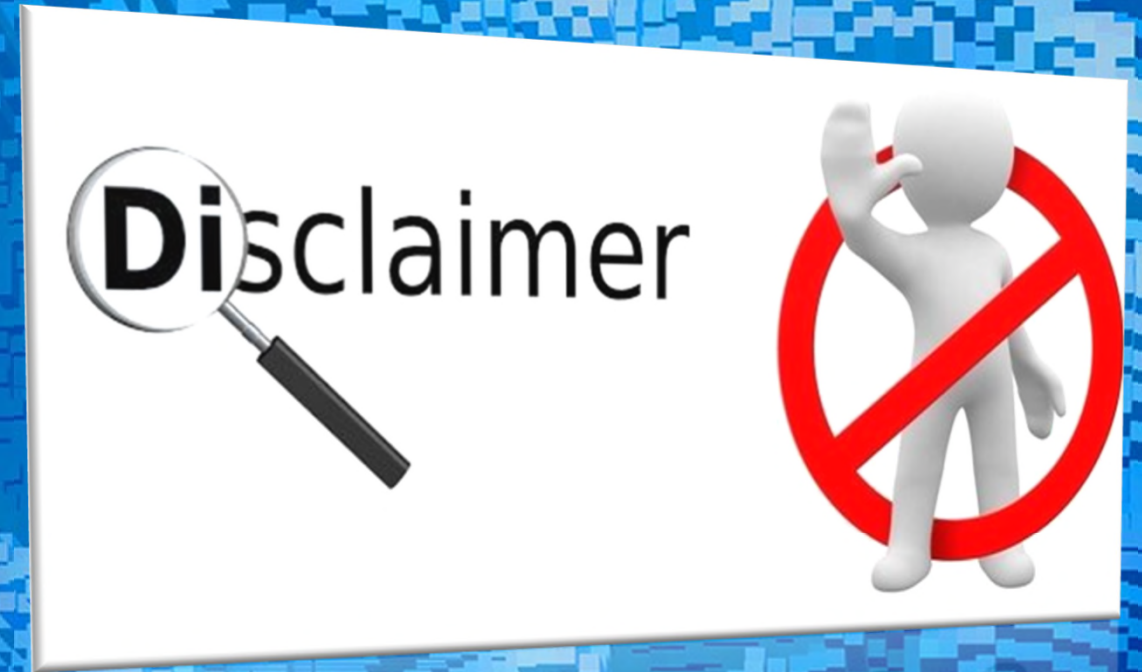
NIKKI ABRAMS



THEM ALL
but we owe

Disclaimer

- We are not representing DCSA or the requirements of Insider Threat Reporting
- Our Insider Threat program has not been characterized as industry best practices
- We are only sharing what we have seen work well within our team



What is required by the DoD?



- National Industrial Security Program
 - 32 CRF Part 117
- Insider Threat Program Senior Officials
 - Cleared to the level of the company
- Cleared Individuals
 - Indicators submitted to DoD
 - 13 Adjudicative Guidelines provided by DoD

What is an Insider Threat?

- An incident by an individual who has or once had authorized access to classified or sensitive information, a facility, network, person, or resource of your company.
- The individual wittingly or unwittingly committed an act in contravention of law or policy which resulted in or might result in harm through the loss or degradation of government or company information, resources, or capabilities. This also includes destructive acts, which may cause physical harm to another in the workplace.



What Is the Threat?

■ What is a threat from the inside?

- A threat to an organization's security or data that comes from within
- Could be an employee, former employee, contractor or business associate
- Threat may involve fraud, theft of confidential or commercially valuable information
- Theft of IP, or sabotage of computer systems
- The threat may also be in the form of violence

■ Why is insider threat more of a concern now?

- Increased number of people with access to sensitive information
- Ease of transferring information electronically
- Growing demand for information from hostile sources
- Importance of unclassified information
- Increased workplace violence and use of weapons



What do insider indicators show?

- What to look for – no easy answer
 - Unethical or criminal behavior
 - Dissatisfaction with the Government or the Company
 - Indicators of alcohol or drug dependencies
 - Unexplained financial affluence or difficulties
 - Misuse of IT technology
 - Unexplainable unusual or odd working hours
 - Seeking information beyond job requirements



Sometimes subtle indicators are all we have, to know someone needs help

Why is Insider Threat Detection so Hard

- People don't display their emotions in public
- People don't want to call attention to themselves
- People are afraid of the consequences
- Indicators aren't obvious
- Co-workers like to explain indicators away
- Co-workers don't want to snitch
- Managers don't want to get a valued employee fired



Small indicators maybe all we have

Myths

- Employee will lose their clearance

Reports are fully vetted by DoD, they apply the whole person concept to any report

- The Employee will be fired

Mercury will do a full investigation, we want to keep valued employees

- Nothing will get done

Our program is about helping people get back on track

- What if I am wrong will I get in trouble for false reports

Your concerns are important all reports are fully investigated

- Everyone will know

All reports are strictly private

Marrian Webster Dictionary – Myth: an unfounded or false notion

Case Study

- Massachusetts-based American Superconductor AMSC
 - Partnered with Chinese company Sinoel to harness wind power
 - AMSC supplied software; Sinoel provided hardware
 - Sinoel began turning away deliveries early in the contract
 - Refused to pay \$100 million owed
 - Cancelled \$800 million in future orders ready to ship
 - Sinoel got access to AMSC intellectual property (Source Code)
- Dejan Karabasevic – AMSC employee
 - Created software for Sinoel using AMSC source code
 - One of only three engineers with access to AMSC source code
 - One of the few engineers to travel to Sinoel (China) often



How did this happen?

- What was known about Karabasevic
 - Having personal problems, including financial difficulties
 - Recently demoted at work
 - Narcissistic personality
 - He was embedded with Sinovel in China
- Sinovel
 - Promised Karabasevic a 5-year, \$1.7 million contract
 - Obtained and used stolen source code
 - Stopped buying from AMSC
- AMSC
 - AMSC stock fell >50% within a month, ultimately losing >95% of its value
 - Revenue fell by >80%
 - AMSC let go >60 % of its work force



Karabasevic: All the warning signs were there...

- They knew he was demoted, though the company still embedded him with a potential hostile client.
- John W. Vandreuil, the U.S. attorney in Madison, Wisc., called Sinovel's attack on American Superconductor, "nothing short of attempted corporate homicide".



If You See Something, Say Something

So, what has Mercury done to assess Insider Trust Indicators?

- Established an Insider Trust team between HR, IT Security and Corporate Security
 - Builds team dynamic while sharing trust, knowledge, resources and meeting regularly
 - Employee are the cornerstone of Mercury Secured Program
- Developed/launched repository to report employee indicators
 - Identified 18 behaviors to consider for reporting
 - Branded as “The Shield”
 - HR, IT Security and Security input data into The Shield
 - Site access to site information only; protect business need to know
 - Threat level guidelines/assessment
 - Developed The Shield training program
 - Established Super User Group



Roles and Responsibilities

- Site Management
- Human Resources
- IT Security
- Facility Security Officer
- First Line Management
- Insider Threat Senior Program Official



If you See Something Say Something to your FSO or HRBP

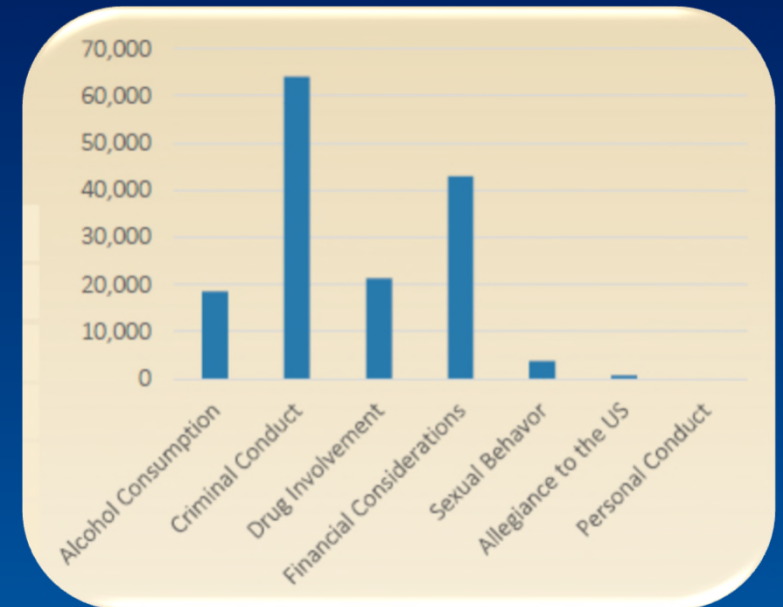
Insider Trust Indicators

13 ADJUDICATIVE GUIDELINES

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Considerations
- Criminal Conduct
- Handling protected Information
- Outside Activities
- Use of Information Technology

MERCURY ADDED INDICATORS

- Performance Improvement Plan
- Resignation
- Identified on Reduction in Force (RIF) list
- Aggressive or Agitated Behavior
- Attempts to Access Restricted Data



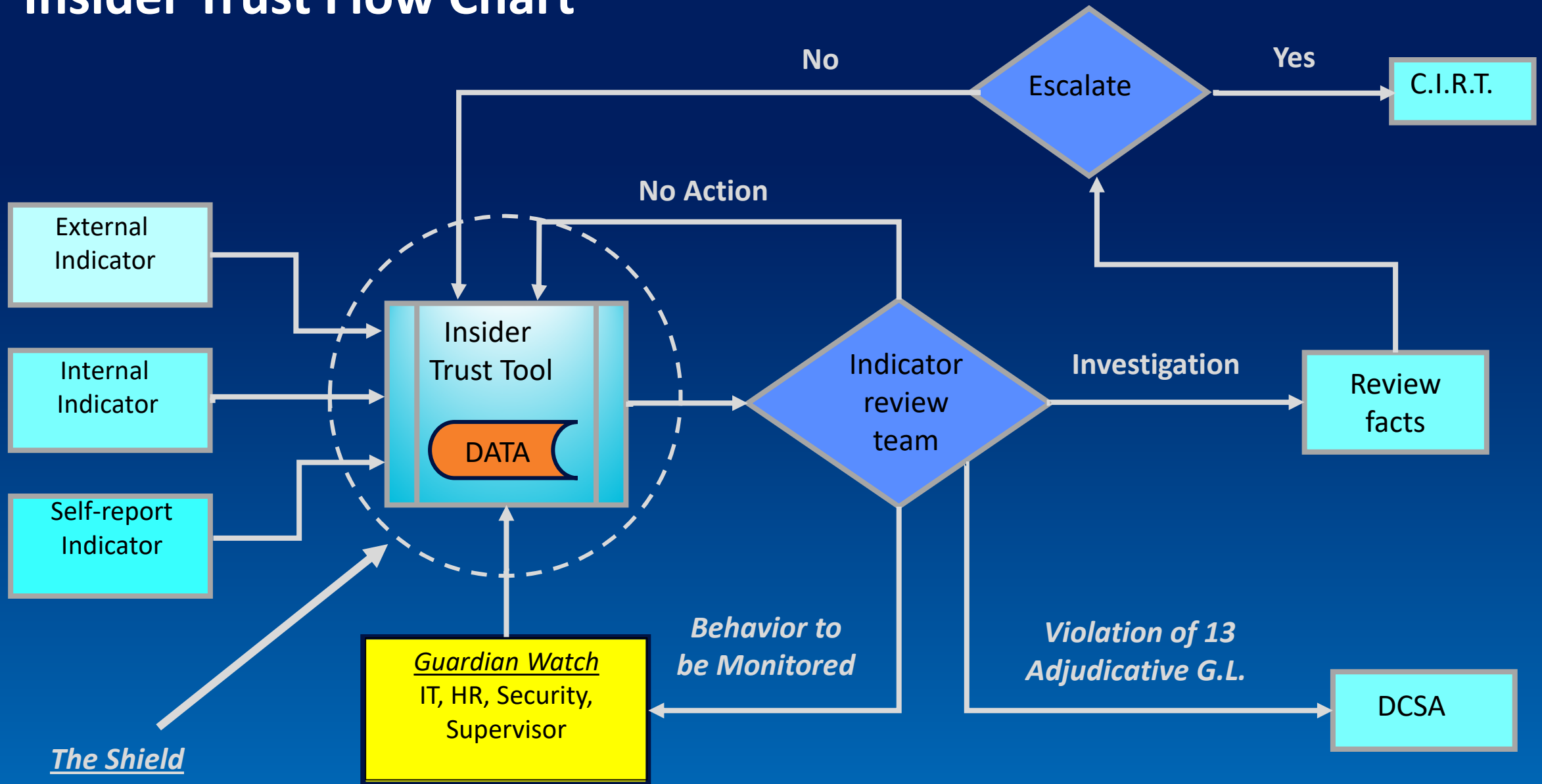
Vetting Risk Operations Center (VROC)

The Shield




- It is a homegrown Program/Tool
- Core Divisions which make up the Super User Team:
 - HR
 - IT Security
 - Corporate Security
- Within the first six months of The Shield being active over 200 reports were reviewed

Insider Trust Flow Chart



Insider Trust Report Entry


Insider Threat Report Number ITRN-20210824T191420920Z

Name * 
If name cannot be found in the directory please enter the information in the "Other Name" field below.

Other Name

Employee Title *

Clearance Level ▼

Effective Date 

Reported By *

Site * ▼

Severity * ▼

Situation Type * Aggressive or agitated behavior ▼

Comments *

Severity * **High**
Medium
Low

Situation Type * **Aggressive or agitated behavior**
Alcohol Consumption
Allegiance to the United States
Attempts to access data not consistent with employment role
Criminal Conduct
Drug Involvement
Financial Considerations
Foreign Influence
Foreign Preference
Identified on a Reduction in Force (RIF)
Involuntary Reduction in Force (RIF)
Involuntary Termination
Minor security violation (no loss/no compromise)
Outside Activities
Performance Improvement plan (PIP)
Personal Conduct
Psychological Conditions
Resignation
Sexual Behavior
Use of Information Technology

How can Excel can help your program?

A	B	C	D	E
Name	Severity	Indicator	Site	Date of pull
Employee G	Medium	Minor security violation (no loss/no compromise)	Site C	10/20/2018
Employee C	Low	Use of Information Technology	Site C	6/18/2019
Employee K	High	Criminal Conduct	Site C	2/24/2020
Employee D	Low	Use of Information Technology	Site D	3/3/2020
Employee A	Low	Use of Information Technology	Site A	6/18/2020
Employee J	Low	Involuntary Termination	Site B	7/4/2020
Employee E	Medium	Aggressive or agitated behavior	Site A	7/17/2020
Employee F	Low	Foreign Influence	Site B	7/17/2020
Employee A	Low	Minor security violation (no loss/no compromise)	Site D	7/24/2020
Employee I	Low	Resignation	Site A	9/3/2020
Employee E	Low	Involuntary Reduction in Force (RIF)	Site A	11/1/2020
Employee B	Low	Resignation	Site B	11/18/2020
Employee M	Low	Resignation	Site A	1/5/2021
Employee Q	High	Involuntary Reduction in Force (RIF)	Site C	3/6/2021
Employee P	Low	Performance Improvement plan (PIP)	Site D	5/6/2021
Employee L	Low	Use of Information Technology	Site D	7/23/2021
Employee A	Low	Resignation	Site B	7/30/2021
Employee O	Low	Resignation	Site C	8/6/2021
Employee B	Medium	Involuntary Reduction in Force (RIF)	Site D	8/6/2021

G	H	I	J	K
Indicator	(All) ▾			
Count of Severity	Column Label			
Row Labels	High	Low	Medium	Grand Total
Employee A		3		3
Employee B		1	1	2
Employee C		1		1
Employee D		1		1
Employee E		1	1	2
Employee F		1		1
Employee G			1	1
Employee I		1		1
Employee J		1		1
Employee K	1			1
Employee L		1		1
Employee M		1		1
Employee O		1		1
Employee P		1		1
Employee Q	1			1
Grand Total	2	14	3	19

How do you start?

CRAWL

- Get Leadership Support
- Pick Core Team
- Develop a Plan
- Set Milestones

WALK

- Enhance your Plan/Program
- Hold Focus Group Meetings

RUN

- Launch your Program
- Launch your Training
- Teach and Learn



mercury



QUESTIONS

Contact Information:

- Paul Fitzpatrick
Paul.Fitzpatrick@mrcy.com
- Nikki Abrams
Nikki.Abrams@mrcy.com

THANK YOU.

mercury

mercy.com

FOLLOW US ON SOCIAL

