Insider Threat

John E. Landers, Ph.D.

Clinical Psychologist

PNNL SA-91626

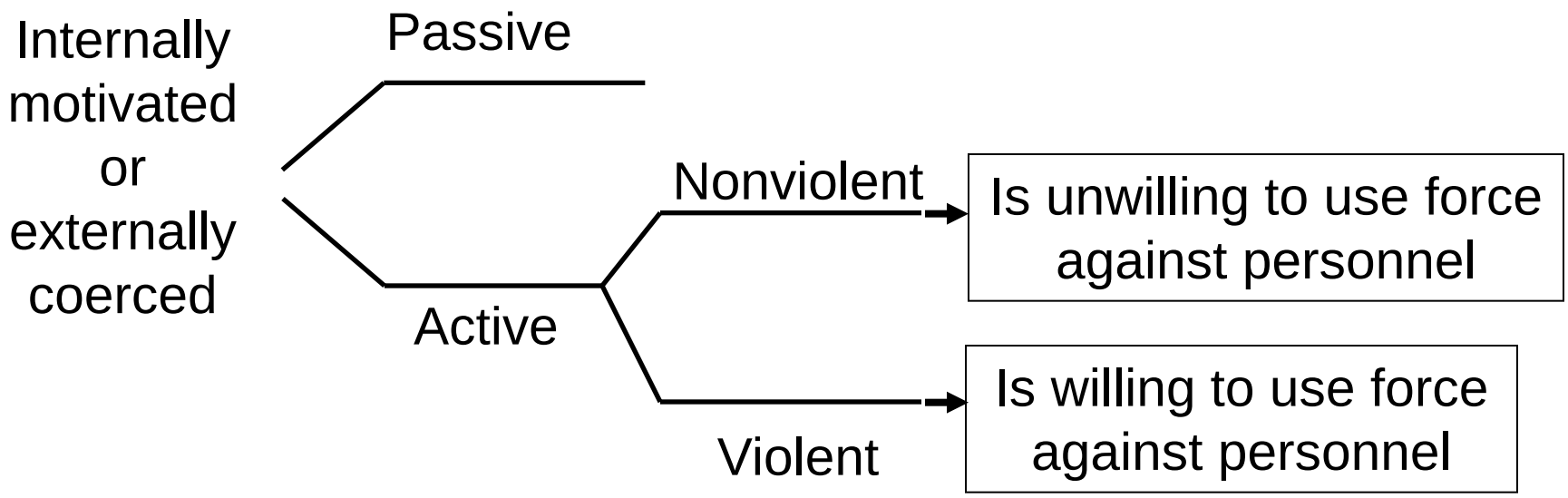
Insiders

- **Insiders represent formidable threats:**
  - **they can often circumvent system elements**
  - **they interact directly with the target without being detected**
- **The delay and detection timelines are not as relevant because insiders can choose the most opportune times and optimum strategies**
- **Insiders can roll-up materials (acquire multiple smaller attractive target materials to equal a Category I quantity) to acquire a goal quantity**

Insider Definition

- **Any individual with access to, knowledge of, and authority over *nuclear facilities* or *transportation of materials* who might attempt unauthorized removal or sabotage, or who could aid *outsiders* to do so.**
- **Insiders might include:**
  - **Management**
  - **Regular employees**
  - **Security personnel**
  - **Service providers**
  - **Visitors**
  - **Inspectors**
  - **Past employees**
  - **Others?**

Insider Categories



- All insiders can use stealth and deceit
- Violent insiders may be rational or irrational

Insider Motivations

- **Ideological – fanatical conviction**
- **Financial – wants / needs money**
- **Revenge – disgruntled employee or customer**
- **Ego – “look what I am smart enough to do”**
- **Psychotic – mentally unstable but capable**
- **Coercion – family or self threatened**

Motivation an important indicator for both level of malevolence and likelihood of attempt

Insider / Outsider Collusion

- **An insiders' access, knowledge, and authority combined with outside resources and skills**
  - **Insider can remove delay elements for outsiders**
  - **Insider can move target partially along path, to be collected by outsiders**
  - **Insider can defeat detection elements (*i.e.,* CAS operator ignores alarms, maintenance technicians bypass sensors, etc.)**
  - **Insider can defeat access controls for outsiders (*i.e.,* vouches for outsiders, escorts outsiders past barriers, etc.)**

Insider Advantages

- Time
  - Can select optimum time to implement plan
  - Can extend acts over long periods of time
- Tools
  - Has capability to use tools and equipment at work location
  - Can attempt to introduce new tools as necessary
- Tests
  - Can test the system with normal “mistakes”
  - Collusion
  - May recruit / collude with others, either insiders or outsiders

Insider can exploit these unique capabilities

Insider Access

- Authorized work areas
- Special temporary access
- Escorted or unescorted
- Emergency access (fire, medical, police, etc.)
- Unauthorized access
- Duration of target exposure
- Protection equipment and process tools
- Special site equipment

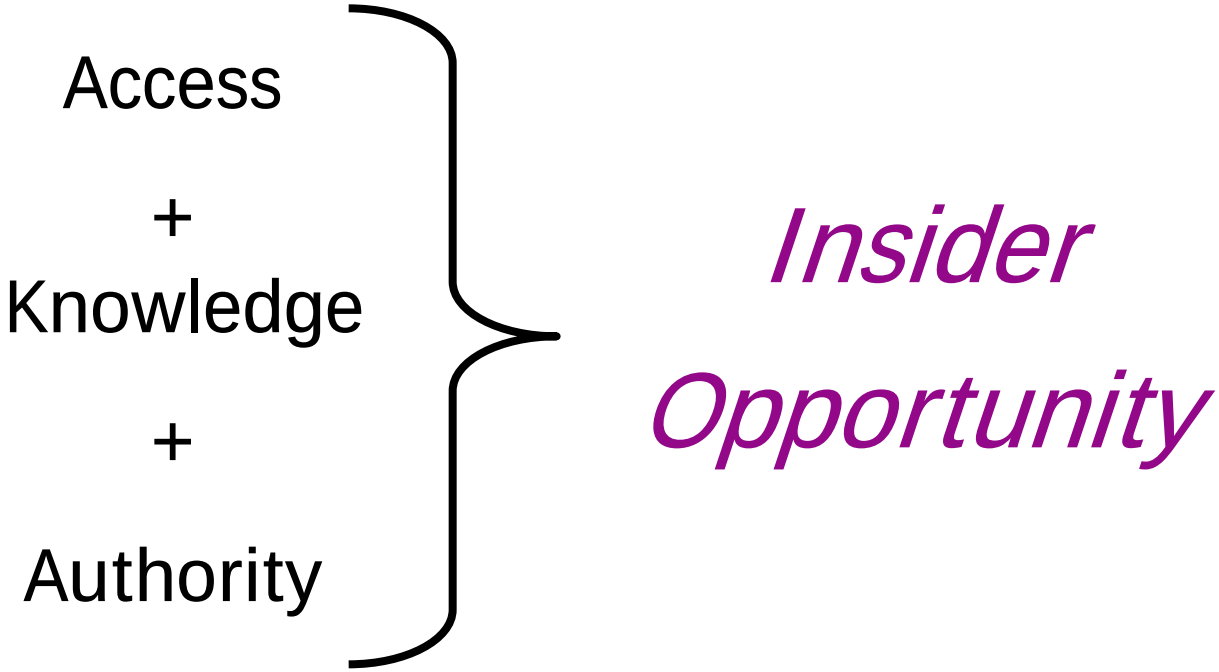
Insider Knowledge

- Targets
  - Locations, characteristics, and details of targets
  - Details of facility layout
- Security systems
  - Security forces capabilities and communications
  - Details of facility and security operations
  - Location and details of safety and security protection systems
- Operations and processes
  - Materials accounting
  - Operational processes
  - Tools and equipment

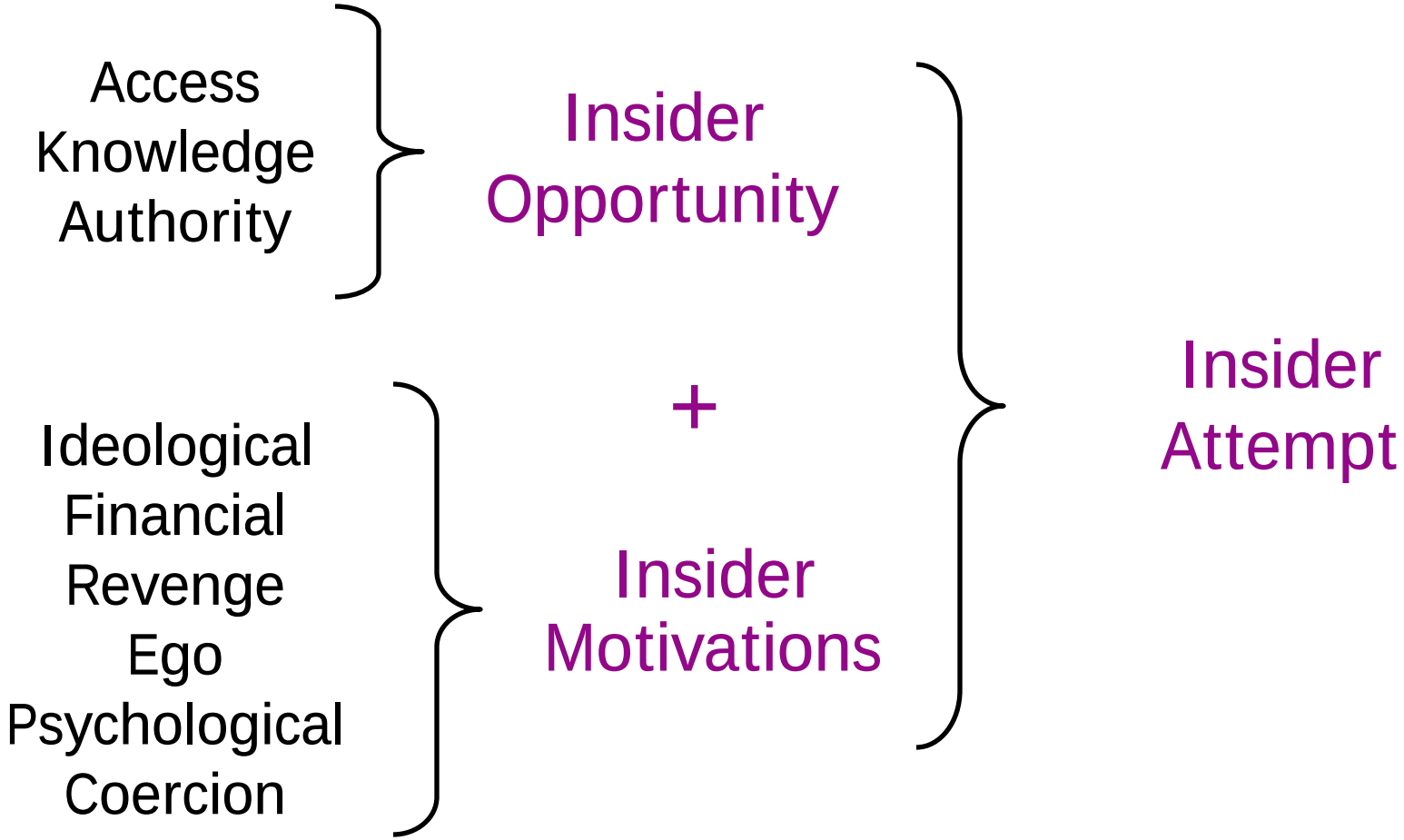
Insider Authority

- Authority over people
  - Designated authority over others
  - Personal influence over others
- Authority over tasks and equipment
  - Assessment of alarms
  - Preparation of sensitive forms
  - Authorization of processes and procedures
- Temporary authority?
- Falsified authority?
- Exemption from procedures?

Opportunity



Factors Affecting Unauthorized Insider Actions



Insider Definition Summary

- Likelihood of unauthorized action
  - Motivation
  - Opportunity
- Insider advantages
  - Time
  - Tools
  - Tests
  - Collusion
- Facility insider characteristics
  - Access
  - Knowledge
  - Authority

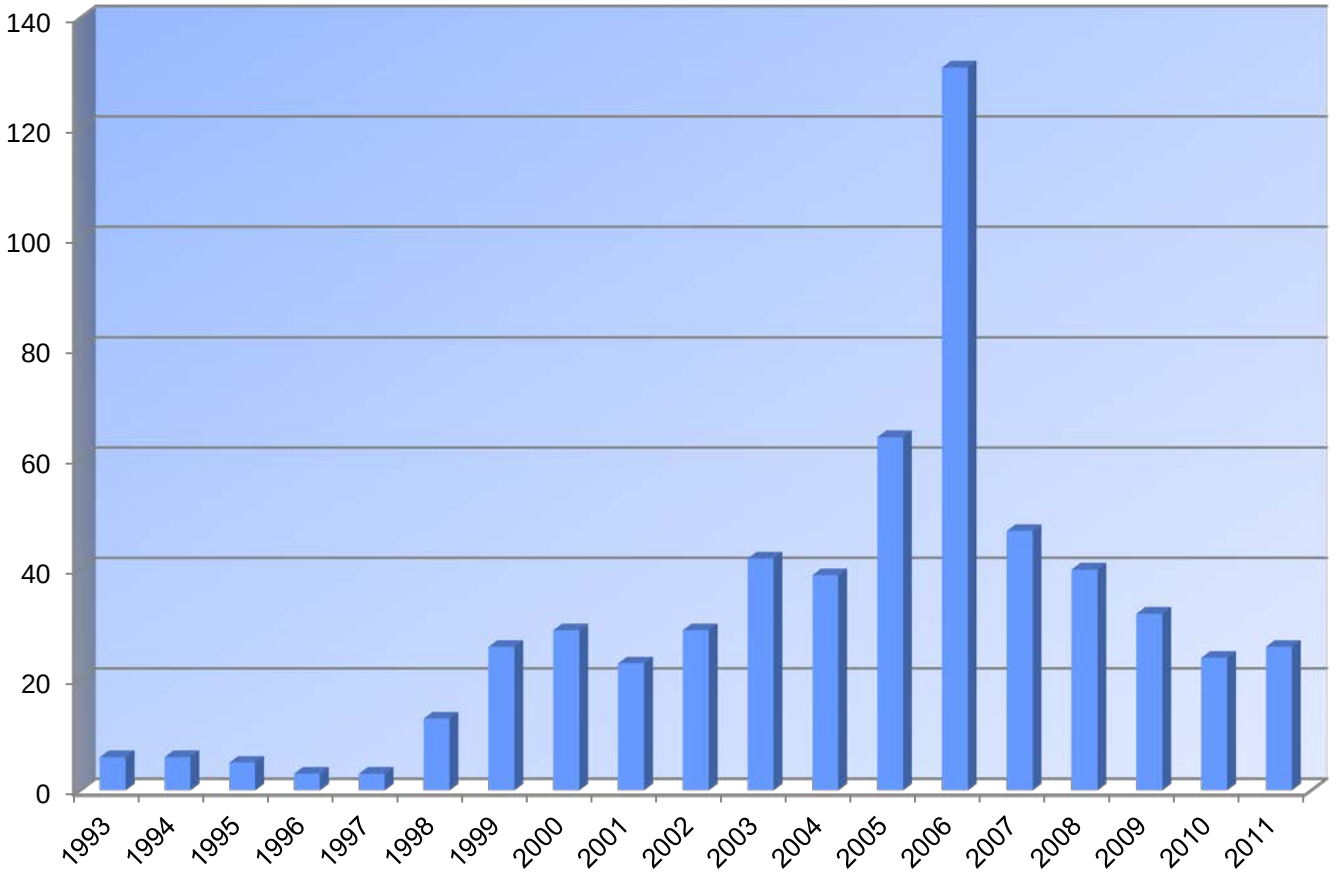
Databases

- **IAEA**
  - **Illicit Trafficking Database (ITDB)**
- **Monterey Institute of International Studies**
  - **Newly Independent States (NIS) Nuclear Trafficking Database**
  - **http://www.nti.org/db/nistraff/index.html**
  - **Database on Nuclear Smuggling, Theft, and Orphan Radiation Sources (DSTO)**

Growing Trends

- **Individual employee of nuclear facility, amateur without connections, motivated by finances (early 1990s)**
- **Groups, using direct routes to terrorists, organized nuclear black market, established underground network (mid and late 90s)**
- **Nuclear community acknowledges demand**
  - **2004, Mohammed al Baradei, chief of the International Atomic Energy Agency, stated it was a "race against time" to prevent terrorists from obtaining nuclear materials.**

ITDB Theft/Loss Incidents 1993-2011



Note: the sharp increase in 2006 is related to a change in reporting procedures, rather than an actual change in incident numbers. The apparent drop from 2009 is a regular phenomenon that has previously been attributable to a reporting time lag of 2–3 years.

Threat is Real

Almost all known cases of theft of nuclear material involved an insider

Nuclear Material Theft - What Do We Know?

- In the 1993–2011 period, 16 confirmed incidents involved unauthorized possession of high enriched uranium or plutonium. Some of these incidents involved attempts to sell or traffic these materials across international borders.
- A small number of these incidents involved seizures of kilogram quantities of potentially weapons-usable nuclear material, but the majority involved gram quantities. In some of these cases, there were indications that the seized material was a sample from a larger unsecured stockpile.
- Incidents involving attempts to sell nuclear materials or radioactive sources indicate that there is a demand for such materials on the 'black market'.
- Amateurish character and poor organization have been the characteristics of many trafficking cases; well-organized, professional and demand-driven trafficking is much more difficult to detect.
- Indication that financial gain is the principal motive behind most events. Some cases, however, showed an indication of malicious intent.

Rivne Nuclear Power Plant - Ukraine, April 2004

- **Four employees of the Rivne NPP in Ukraine bribed a security officer working at the plant's checkpoint to pass through security and stole a spare reactor evaporator heating chamber.**
- **The thieves paid the security officer 400 hryvnyas (or US $77) for the service.**
- **The thieves sold the stolen piece of equipment as local scrap metal for a mere 1,600 hryvnyas (or US $309). Experts estimated its cost at 800,000 hryvnyas (or US $154,000).**

IAEA Organized Crime Study (2001 – 2005) Conclusions

- Groups were engaged in buying, selling, or storing radioactive substances, including nuclear fissile material.
- Detection of activity typically as a result of a tip-off that radioactive material was being offered for sale.
- 60% of these organized criminal networks were of transnational character insofar as they either involved actors of various nationalities or dealt internationally.
- In most cases, motivation is financial.

Insider Threat Data - Conclusions

- **The Threat is Real.**
- **Trusted individuals with access to information and/or nuclear material have been involved with almost all of these incidents.**

Appendix A

IAEA ITDB Records of HEU and Pu Trafficking

ITDB (IAEA) Records of HEU and Pu Incidents from 1993

Date	Location Detected	Material Involved	Incident Description
1993-05-24	Vilnius, Lithuania	HEU/ 150 g	4.4 t of beryllium including 140 kg contaminated with HEU were discovered in the storage area of a bank.

ITDB (IAEA) Records of HEU and Pu Incidents in 1994

Date	Location Detected	Material Involved	Incident Description
1994-03	St. Petersburg, Russian Federation	HEU/ 2.972 kg	An individual was arrested in possession of HEU, which he had previously stolen from a nuclear facility. The material was intended for illegal sale.
1994-05-10	Tengen-Wiechs, Germany	Pu/ 6.2 g	Plutonium was detected in a building during a police search.
1994-06-13	Landshut, Germany	HEU/ 0.795 g	A group of individuals was arrested in illegal possession of HEU.
1994-07-25	Munich, Germany	Pu/ 0.24 g	A small sample of PuO2-UO2 mixture was confiscated in an incident related to a larger seizure at Munich Airport on 1994-0810.
1994-08-10	Munich Airport, Germany	Pu/ 363.4 g	PuO2-UO2 mixture was seized at Munich airport.
1994-12-14	Prague, Czech Republic	HEU/ 2.73 kg	HEU was seized by police in Prague. The material was intended for illegal sale.

ITDB (IAEA) Records of HEU and Pu Incidents in 1995

Date	Location Detected	Material Involved	Incident Description
1995-06	Moscow, Russian Federation	HEU/ 1.7 kg	An individual was arrested in possession of HEU, which he had previously stolen from a nuclear facility. The material was intended for illegal sale.
1995-06-06	Prague, Czech Republic	HEU/ 0.415 g	An HEU sample was seized by police in Prague.
1995-06-08	Ceske Budejovice, Czech Republic	HEU/ 16.9 g	An HEU sample was seized by police in Ceske Budejovice.

ITDB (IAEA) Records of HEU and Pu Incidents in 1999

Date	Location Detected	Material Involved	Incident Description
1999-05-29	Rousse, Bulgaria	HEU/ 10 g	Customs officials arrested a man trying to smuggle HEU at the Rousse customs border check point.
1999-10-02	Kara-Balta, Kyrgyzstan	Pu	Two individuals were arrested trying to sell Pu.

ITDB (IAEA) Records of HEU and Pu Incidents in 2000

Date	Location Detected	Material Involved	Incident Description
2000-04-19	Batumi, Georgia	HEU/ 770 g	Four individuals were arrested in possession of HEU.
2000-09-16	Tbilisi Airport, Georgia	Pu/ 0.4 g	Nuclear material including Pu was seized by police in Tbilisi Airport.
2000-12	Karlsruhe, Germany	Pu/ 0.001 g	Mixed radioactive materials including a minute quantity of plutonium were stolen from the former pilot reprocessing plant.

ITDB (IAEA) Records of HEU and Pu Incidents in 2001

Date	Location Detected	Material Involved	Incident Description
2001-01-28	Asvestochori, Greece	Pu/ ~3 g	245 small metal plates containing Pu were found in a buried cache in the Kouri forest near the Asvestochori village.
2001-07-16	Paris, France	HEU/ 0.5 g	Three individuals trafficking in HEU were arrested in Paris. The perpetrators were seeking buyers for the material.

ITDB (IAEA) Records of HEU and Pu Incidents in 2003

Date	Location Detected	Material Involved	Incident Description
2003-06-26	Sadahlo, Georgia	HEU/ ~170 g	An individual was arrested in possession of HEU upon attempt to illegally transport the material across the border.

ITDB (IAEA) Records of HEU and Pu Incidents in 2005

Date	Location Detected	Material Involved	Incident Description
2005-03 to 2005-04	New Jersey, USA	HEU/ 3.3 g	A package containing 3.3 g of HEU was reported lost.
2005-06-24	Fukui, Japan	HEU/ 0.0017 g	A neutron flux detector was reported lost at an NPP.

Detecting the Malicious Insider through Behavioral Science

John E. Landers, Ph.D.

Clinical Psychologist

PNNL SA 91626

Focusing on Predicting Risk vs. Predicting Behavior

Accurately Predicting The Insider Threat

		Reality of Threat	
		+	-
Screening Tool	+	true positive	false positive
	-	false negative	true negative

Accurately Predicting The Insider Threat

If we minimize

This is greater

		Reality of Threat	
		+	-
Screening Tool	+	true positive	false positive
	-	false negative	true negative

Behavioral Science Prediction Terminology

- **Selection Ratio - the number of positions of trust divided by the number of individuals who applied for these positions of trust.**
- **Base Rate - prevalence of target problem (e.g., espionage) in a specific population (e.g., workers) to be screened.**

Behavioral Science Prediction Terminology

- **Sensitivity - the proportion of true positives that are actually detected by a screening test.**
- **Specificity - the proportion of true negatives that are actually detected by a screening test.**
- **Accuracy - the percent of cases in which a screening test correctly predicts reality. High accuracy requires high sensitivity and high specificity.**

Example 1: Proportion of employees who will be threat = .50 (Base rate)

	Selection Ratio			
Accuracy	.10	.30	.50	.90
.00	.50	.50	.50	.50
.25	.67	.62	.58	.52
.50	.84	.74	.67	.54
.95	1.00	.99	.90	.56

Example 2: Proportion of employees who will be threat = .20 (Base rate)

	Selection Ratio			
Accuracy	.10	.30	.50	.90
.00	.20	.20	.20	.20
.25	.34	.29	.26	.21
.50	.52	.38	.31	.22
.95	.97	.64	.40	.22

Understanding Science of Prediction – Accuracy

- When accuracy = .00, using the test results in a success rate equal to the base rate, which is the same thing as not using the test
- As accuracy increases, the test utility increases
- An accuracy value of .4 is considered high

Understanding Science of Prediction – Selection Ratio

- When the selection ratio is small, increases in accuracy significantly increase test utility
- When the selection ratio is large, accuracy makes little difference and there is little test utility. This happens because we cannot be selective
- Occupations having significant aptitude, experience, training, etc… naturally decrease applicant pool and increase selection ratio

Understanding Science of Prediction – Base Rate

- When base rates significantly vary from .5, test utility significantly decreases
- Fortunately, base rates for insider threat behavior are low
- Unfortunately, this makes it close to impossible to predict exactly who will be an insider threat with any degree of accuracy

Predicting Risk not Who

- Ultimately, it is going to be impossible to reliably eliminate the insider threat through predicting exactly who will be the insider threat
- Rather, it is a better use of resources to identify risk factors (e.g., security infraction)
- And mitigate risk (e.g., education) based on those factors

Human Reliability Program – Overview

- Federally mandated
- Individuals with access to certain materials, nuclear explosive devices, facilities, and programs
- System of continuous evaluation
- Identifies individuals demonstrating behavioral, psychological, or physical risk factors

Human Reliability Program – Access

- Access to Category I SNM (e.g., responsibility for transportation or protection of material)
- Responsibility for working with, protecting, or transporting nuclear explosives, nuclear devices, or selected components;
- Access to information concerning vulnerabilities in protective systems
- Potential to significantly impact national security or cause unacceptable damage

Human Reliability Program – Screening Process

- A DOE "Q" access authorization, initial and every five years thereafter
- Initial and annual submission of Questionnaire for National Security Positions, and an annual review of the personnel security file
- Signed releases, acknowledgments, and waivers to participate in the HRP
- Completion of initial and annual HRP instruction
- Successful completion of an initial and annual supervisory review, medical assessment, management evaluation, and a DOE personnel security review
- No use of any hallucinogen or flashbacks in the preceding five years
- Initial and annual psychological evaluation
- Initial and annual and random alcohol and drug tests at least once each 12 months
- Initial Polygraph examination

Human Reliability Program – Removal

- HRP manager, physician, psychologist, or security manager may immediately remove participant from HRP duties
- This is a temporary removal that does not impact pay/promotion potential
- Employee given written documentation of reason for removal within 24 hours
- Investigation will lead to reinstatement or permanent removal
- If recommendation is permanent removal, employee has local and federal appeals processes for reinstatement

Human Reliability Program – Purpose

- The purpose for this program is to minimize risk related to malicious insider behavior
- Program provides for protection of employees as process is transparent and has independent appeals process
- Program allows for individuals with access to be temporarily removed and provided with resources to mitigate risk

Case Study - Background

- Long term
- Trusted
- Skilled employee
- Protracted theft of significant quantity of material
- Acted alone

Case Study - Motivation

“I lived from paycheck to paycheck, but it was stable. Then… money lost its value. That was when I got this idea to siphon off uranium little by little.”

“I just needed a new refrigerator and a new gas stove. I didn't need a big profit. I just needed to live through the tough times when I wanted to buy something but couldn't because of inflation. My salary couldn't keep up and I couldn't buy anything. I just needed to buy a few essentials and then work honestly.”

Case Study – Analysis

- Could the organization have predicted this event?
- What were the risk factors?
- How could the organization detect these risk factors?
- How could the organization mitigate these risk factors?

Detection, Deterrence, and Mitigation of Malicious Insider Threat

- Materials Protection
- Materials Control
- Materials Accountability
- Nuclear Security Culture

Importance of Human Factor

“Good security is 20% equipment and 80% people.”

Gen. Eugene Habiger

former Assistant Secretary for Safeguards and Security

U.S. Department of Energy

Measuring and Monitoring NSC

“Until you can measure something and express it in numbers, you have only the beginning of understanding.”

Lord Kelvin

Aberrant Behavior

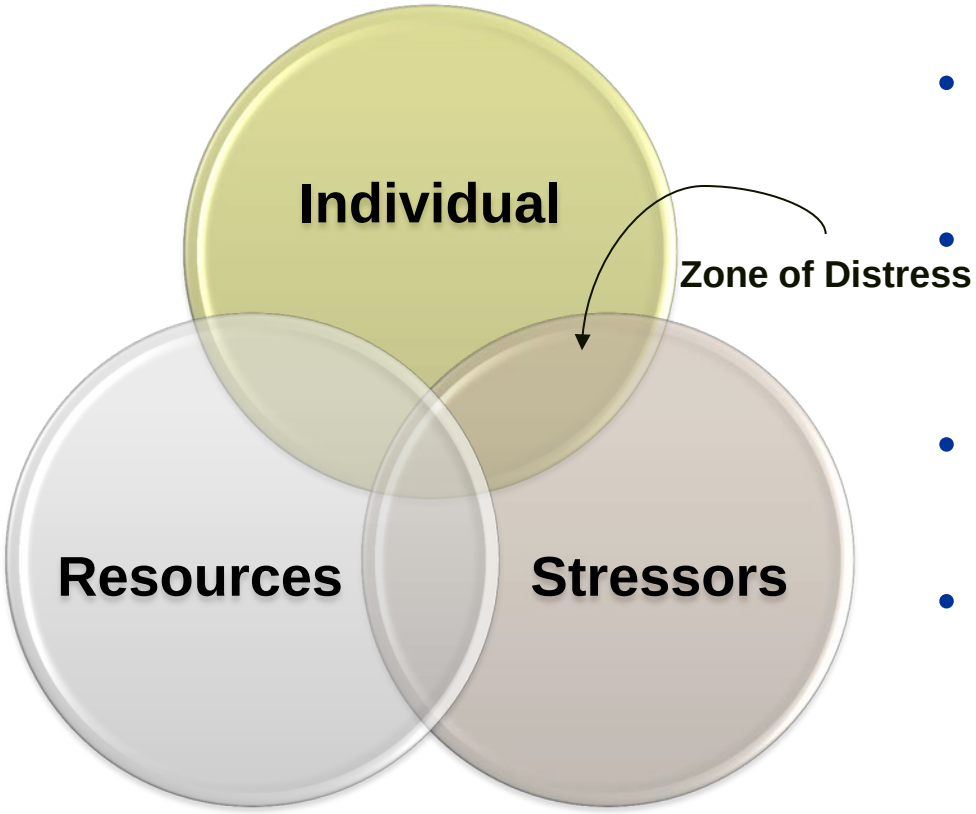
Aberrant behaviors are any characteristics, attitudes or behaviors of individuals, organizations or institutions which serve as a means to undermine nuclear security

Aberrant Behavior

- Additionally, aberrant behaviors have been shown to increase risk of malicious insider behavior
- Understanding origins, recognizing, reporting, and responding to aberrant behaviors are important components of measuring and monitoring NSC

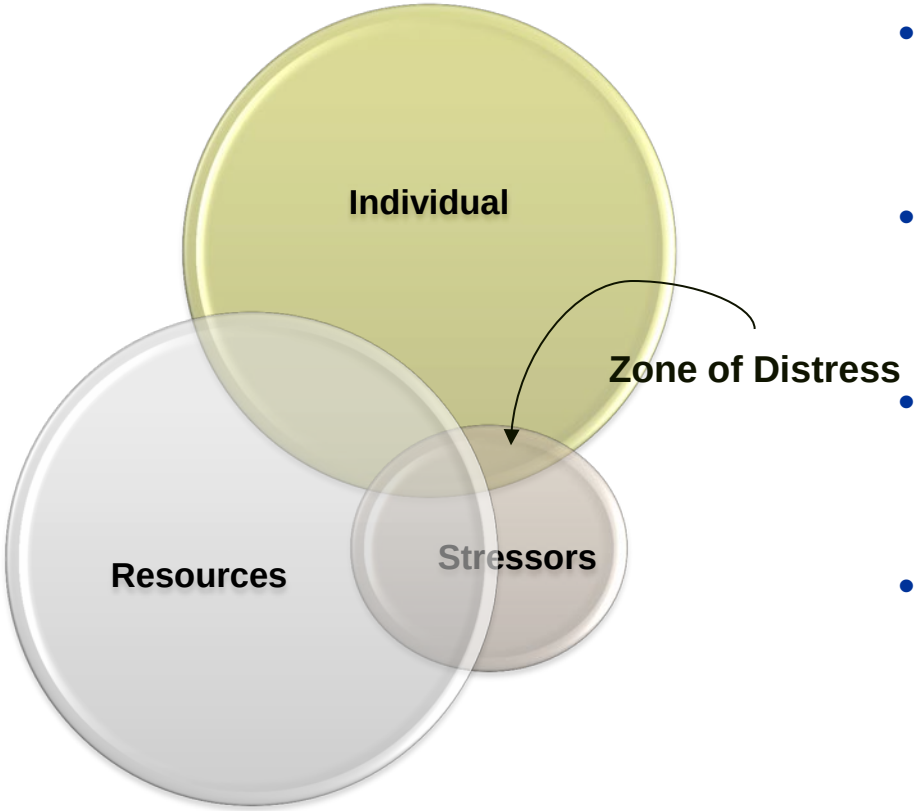
Origins of Aberrant Behavior

Aberrant Behavior Origination Model



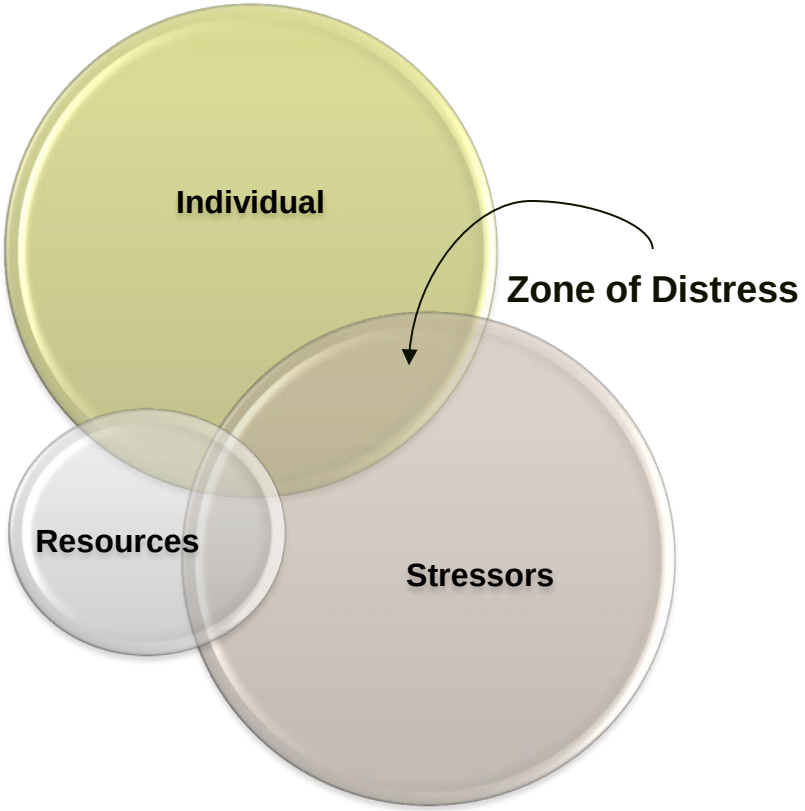
- All individuals experience stressors
- Stressors can be both positive (e.g., marriage) and negative (e.g., divorce)
- To the degree than an individual has access to resources, the impact of stressors is mitigated
- When stressors impact an individual without adequate resources, distress occurs
- Aberrant behavior is the individual's response to chronic distress

Aberrant Behavior Origination Model



- Individuals with adequate resources are less likely to experience distress
- Individuals experiencing fewer stressors are less likely to experience distress
- Examples of external resources are money, social support and secure employment
- Examples of Internal resources are emotional stability, physical health and interpersonal skills

Aberrant Behavior Origination Model



- Individuals with inadequate resources are more likely to experience distress
- Individuals experiencing abnormally high degree of stressors are more likely to experience distress

Common Stressors

- Family Concerns
- Interpersonal Concerns
- Financial Concerns
- Physical Concerns
- Addictive Concerns
- Psychological Concerns
- Workplace Concerns
- Legal Concerns
- Ethical/Moral Concerns

Important Resources to Counteract Stressors

- Positive family relationships
- Strong social support network
- Financial stability & philosophy of living within means
- Good physical health & lifestyle conducive to maintaining physical health
- Abstinence from addictive substances (e.g., alcohol, mind or mood altering prescription medications, illicit drugs) and behaviors (e.g., gambling, pornography, illicit sex)

Important Resources to Counteract Stressors

- History of stable personal and family psychological functioning
- History of positive workplace functioning and relationships with coworkers and supervisors
- History free of arrests or convictions as well as strong commitment to citizenship
- History of behaving with integrity and avoidance of situations that could be compromising or shaming

Organizational Resources

- Loan Program
- Counseling Program
- Family Leave

Recognizing & Reporting Aberrant Behaviors

Keys to Recognition & Reporting

- The keys to recognizing aberrant behaviors are continual observation, recognition of aberrant behaviors, and reporting these observations
- The methods of observation by security vs. the coworker may vary; however, the attitude is the same – one of awareness and concern
- Recognition of aberrant behaviors is only accomplished through initial and regular training that is meaningful and relevant to the managers and employees
- Reporting observations has multiple cultural obstacles that can only be resolved through directly addressing these concerns
- Employee in question is always involved in this process and has protections built into process

Sources of Recognition & Reporting

- Security
- Management
- Psychologist/Medical
- Coworkers
- Self

Security – Recognition & Reporting of Aberrant Behaviors

- Security should do thorough background checks on all applicants for positions of trust, prior to employment
- Background checks should include known risk factors such as financial history, legal history, work history, family history, psychiatric history, etc…
- People exhibiting anything other than low risk should be eliminated from consideration
- Security should always verify all people in positions of trust. Continual checks are necessary to detect changes
- If changes are recognized further evaluation is necessary

Security – Recognition & Reporting of Aberrant Behaviors

- Corrective action plans can be implemented to reduce stressors and bolster resources
- Temporary removal from position of trust may be necessary, depending upon the nature of the concern
- Training employees to recognize and report concerns is a key component of success and is the role of the security department
- Relationships with outside entities (e.g., law enforcement) is also helpful in detecting risk factors

Management – Recognition & Reporting of Aberrant Behaviors

- Managers need to understand they are a key component in detecting aberrant behavior
- Managers should receive initial and annual training regarding their role in the recognition and reporting process
- They are in a position to recognize common aberrant behaviors amongst their employees
- They should immediately report concerns for further evaluation

Management – Recognition & Reporting of Aberrant Behaviors

- They are also in a position to encourage employees in positions of trust to recognize and report concerns regarding themselves and coworkers
- Annual reviews of employee functioning should be completed and sent to psychologist/medical prior to annual evaluation

Psychologist / Medical – Recognition & Reporting of Aberrant Behaviors

- The psychologist /physician should evaluate all candidates for positions of trust prior to hiring and at least annually thereafter
- Employees having demonstrated aberrant behaviors will require more frequent monitoring and evaluation
- The psychologist/physician should have access to the following prior to the evaluation: manager review, security review, psychological/medical testing, self-report of life events
- Initial psychological evaluations should include tests that include measures of abnormal emotional and personality traits as well as ability to detect deception.
- Initial medical evaluations should include full history and physical
- Tests should be re-administered regularly

Psychologist / Medical – Recognition & Reporting of Aberrant Behaviors

- **Annual evaluations should follow a semi-structured interview format that probe the following areas:**
  - **medical**
  - **family**
  - **interpersonal**
  - **financial**
  - **physical**
  - **addictive**
  - **psychological**
  - **workplace**
  - **legal**
  - **ethical/moral concerns**

- **The "client" of the psychologist and physician is the organization, not the person being evaluated.**
- **Conclusions regarding suitability, reliability and judgment of individual should be communicated to security and management**

Coworkers – Detection of Aberrant Behaviors

- Coworkers are the primary means of recognition and reporting and are essential to the success of any culture measurement and monitoring program
- They are in a position to recognize common aberrant behaviors amongst their coworkers
- They should immediately report concerns to management for further review
- Employees in positions of trust must receive initial and regular training thereafter regarding their role in the recognition and reporting process

Coworkers – Detection of Aberrant Behaviors

- Employees may be reluctant to report concerns
  - coworkers are their friends
  - they have worked together for a long time
  - they just don't want to get involved
- Employees will need to be assured that they are the first defense against the insider threat
- Early recognition and reporting through their vigilance may not only prevent security concerns, but may also help salvage a coworker prior to becoming a malicious insider

Importance of Recognition and Reporting Concerns

"If you want to do these people a favor who have problems -- and I'm talking from experience -- say something. If somebody had said something to me and put a block in front of me and said, 'I think Jeff's got a problem and I don't think that he's handling it very well,' that would have been enough to stop the process….I lost everything -- my dignity, my freedom, my self-respect."

Jeff Carney

Convicted American Spy

Self – Detection of Aberrant Behaviors

- Employees have a duty to immediately report taking prescription drugs and over-the-counter remedies that can impair their performance
- Employees also have a duty to immediately report any significant life changing event to the psychologist.
- The psychologist/physician will assess whether this individual is experiencing distress and provide direction and support
- If employees are conscientious in reporting and seeking help for impairing conditions there will be no need for others to report their behavior to officials
- They will likely be able to correct concerns before they impact their career

Enhancing Nuclear Security

- The spirit of the program should be to reward early detection of aberrant behavior and do everything possible to provide necessary resources to employees needing corrective actions in order to ensure rehabilitation
- Managers, security personnel, medical personnel and the psychologist should coordinate efforts and information to ensure the best decisions are made
- Ability to temporarily remove employee from position of trust without loss of pay or promotion potential as a precautionary measure
- Employee is afforded due process

Enhancing Nuclear Security

- An Employee Assistance Program (EAP) administered through Human Resources should be available as a referral source for assistance/counseling for employees (and dependants) in positions of trust demonstrating aberrant behaviors and/or distress
- EAP should be available through self-referral and management referral
- EAP records should remain private, except in cases of risk to self, others, or concerns of imminent risks of national security

Psychological Barriers to Effective Nuclear Security

John E. Landers, Ph.D.

Clinical Psychologist

PNNL SA 91626

National Nuclear Security Administration

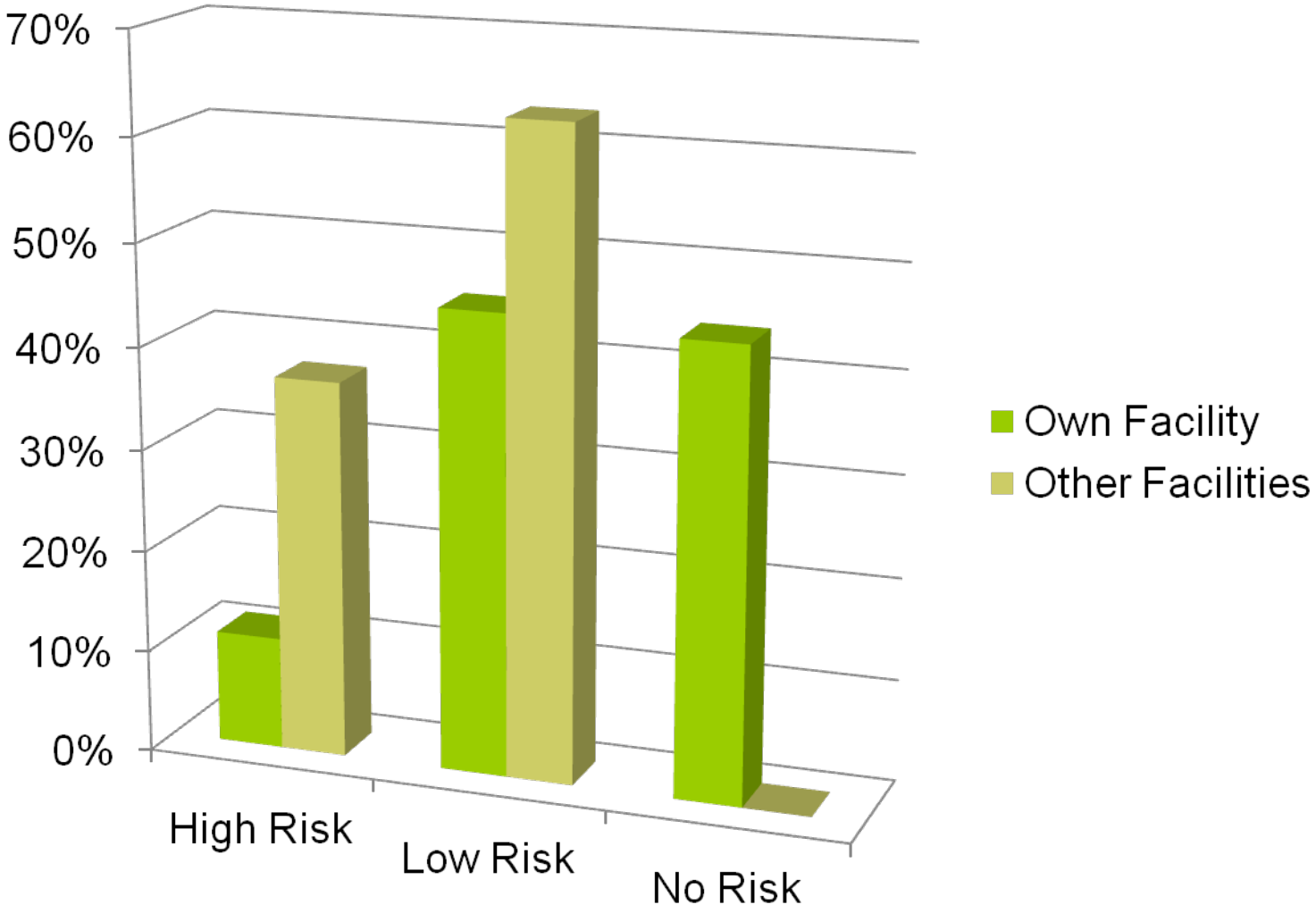
“The greatest discovery of my generation is that a human being CAN alter his life by changing his attitude.”

William James, First American Psychologist

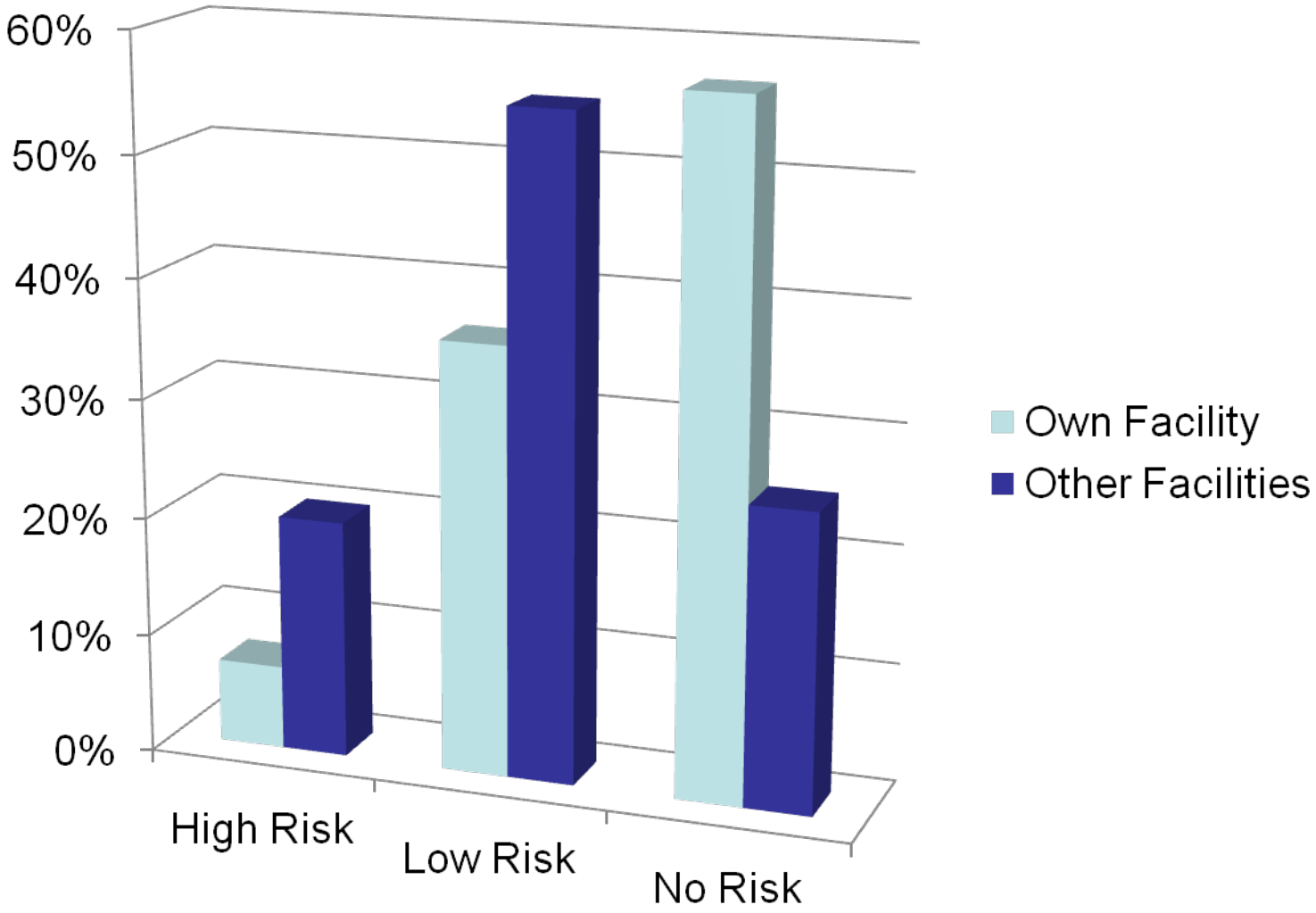
We never talked about an inside threat, only about people outside the collective, about an attack, about war. And now, …we are facing the insider problem."

Gennady Pshakin,
Head of Department, International Relations
Russian Methodological Training Center

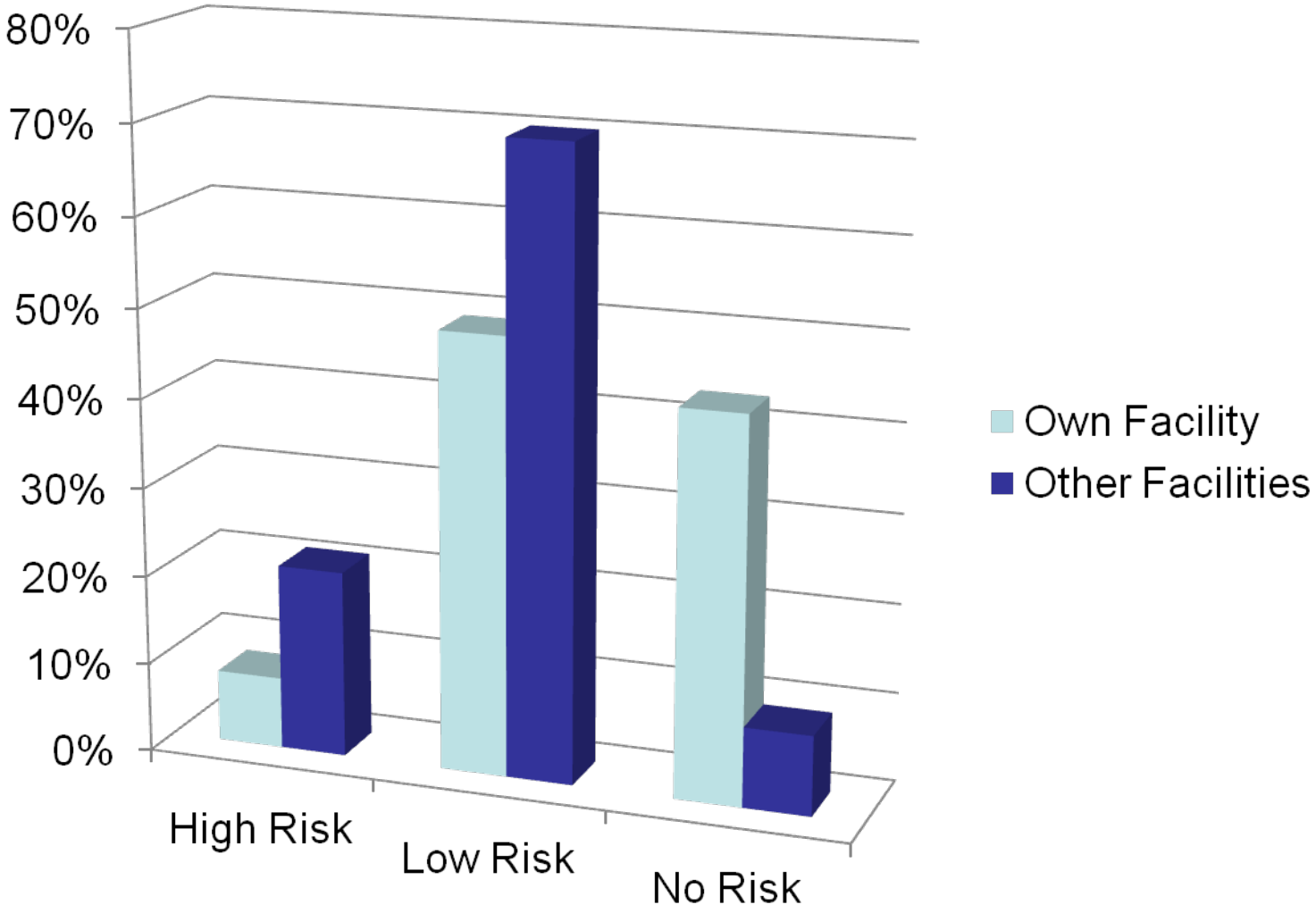
Perception of Vulnerability to Theft or Diversion of NM (Top Level Managers)



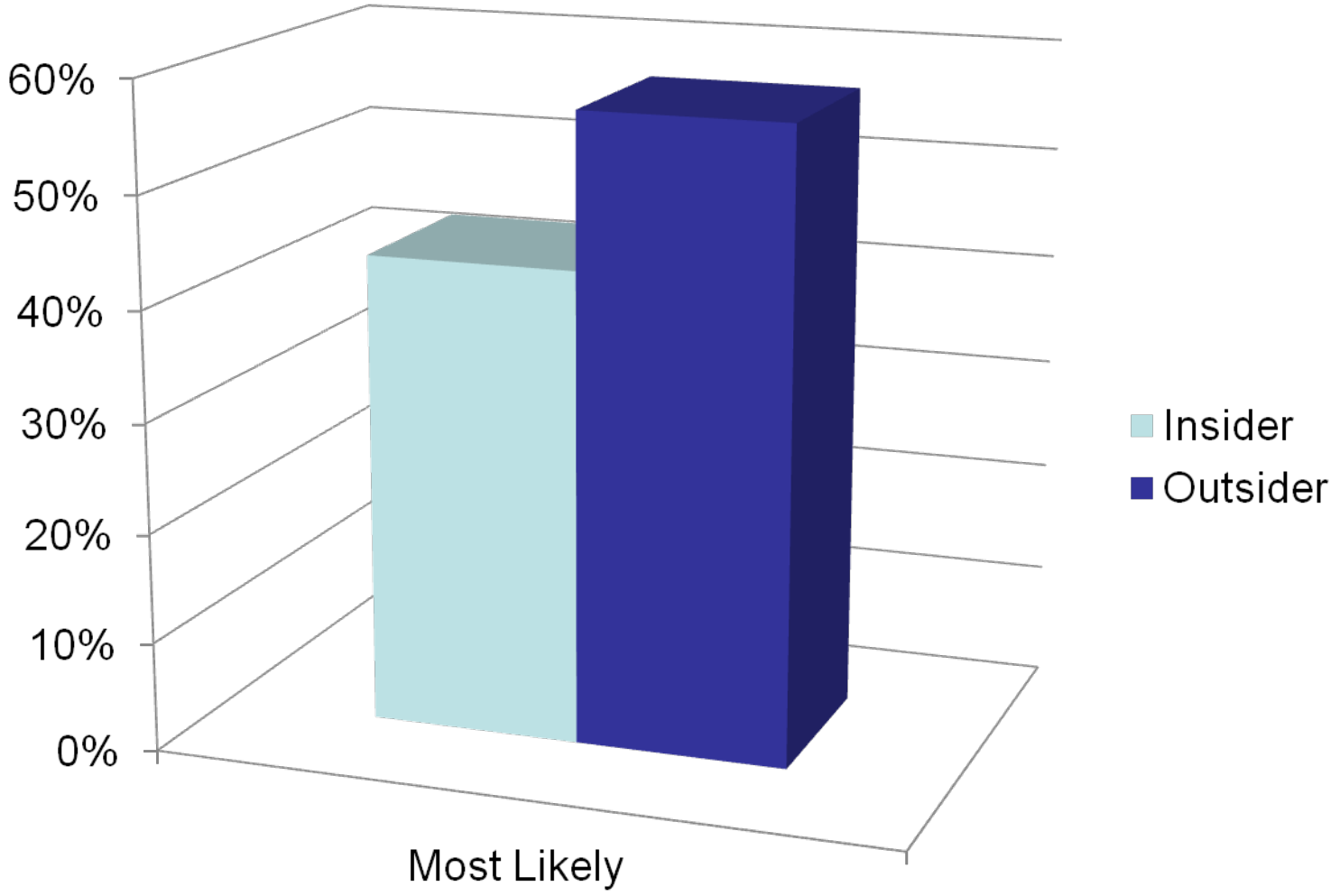
Perception of Vulnerability to Theft or Diversion of NM (Mid-Level Managers)



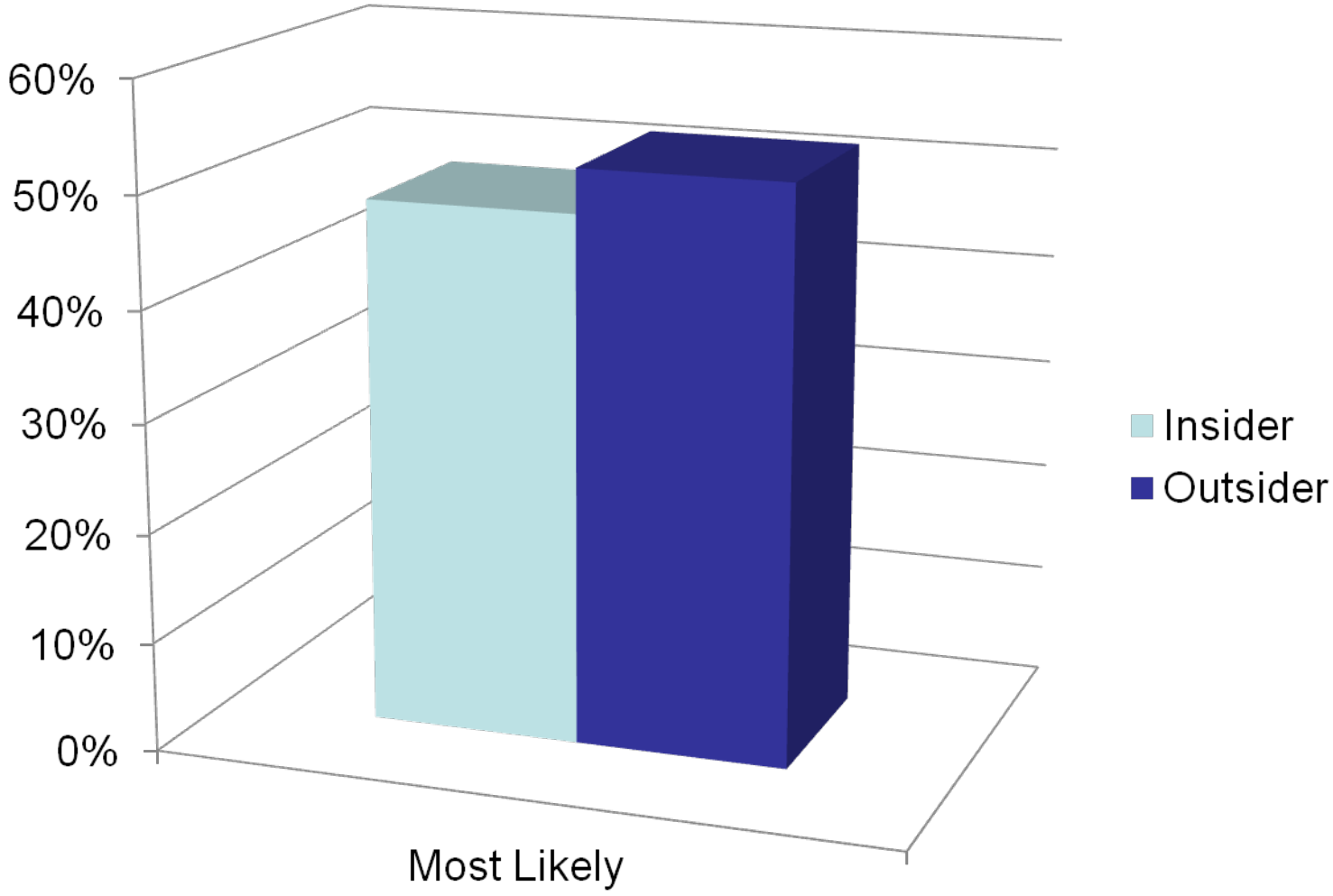
Perception of Vulnerability to Theft or Diversion of NM (MPC&A Employees)



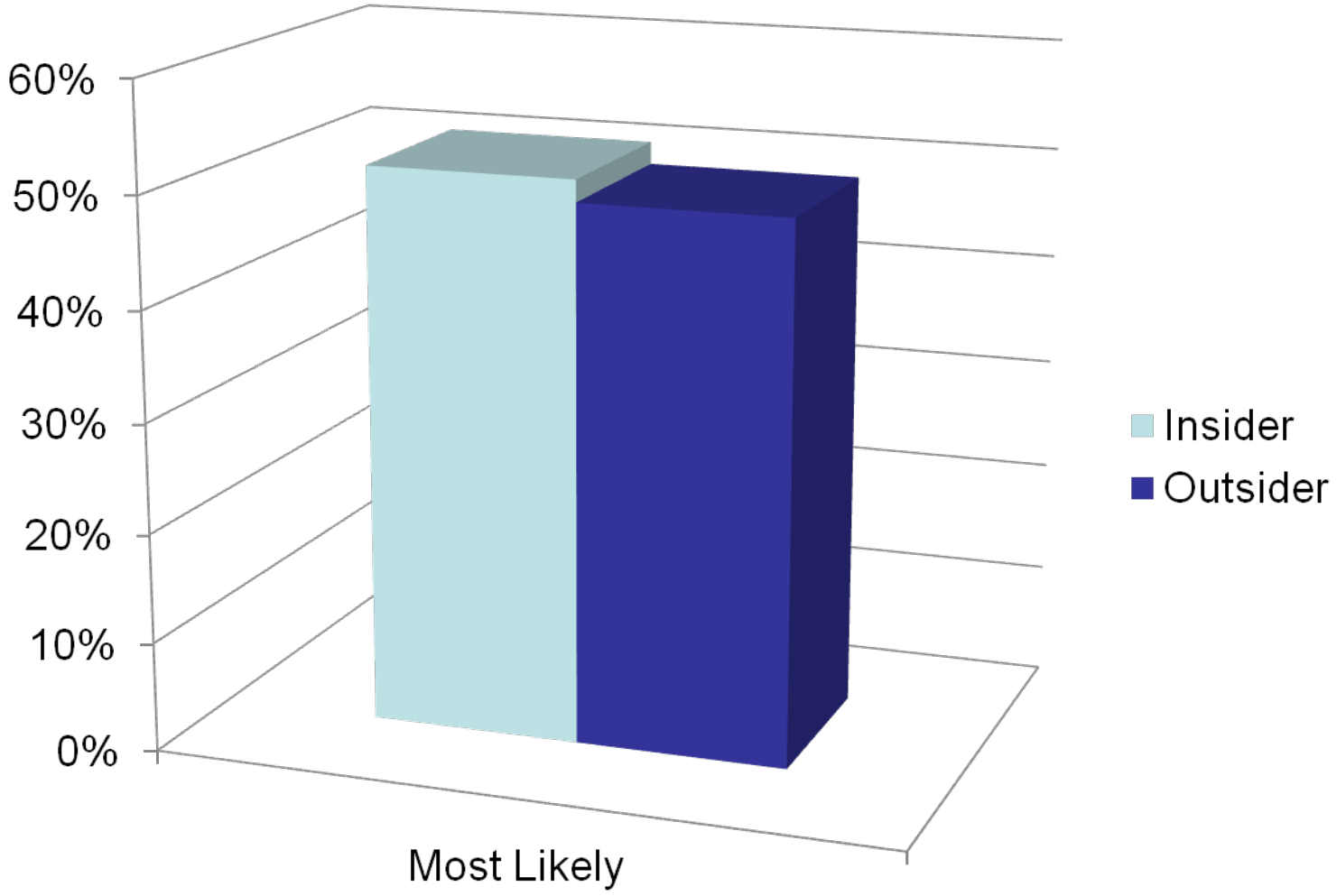
Perception of Insider versus Outsider Risk (Top Level Managers)



Perception of Insider versus Outsider Risk (Mid-Level Managers)



Perception of Insider versus Outsider Risk (MPC&A Employees)



Influencing Behavior

Understanding the Variables

Individual Variables

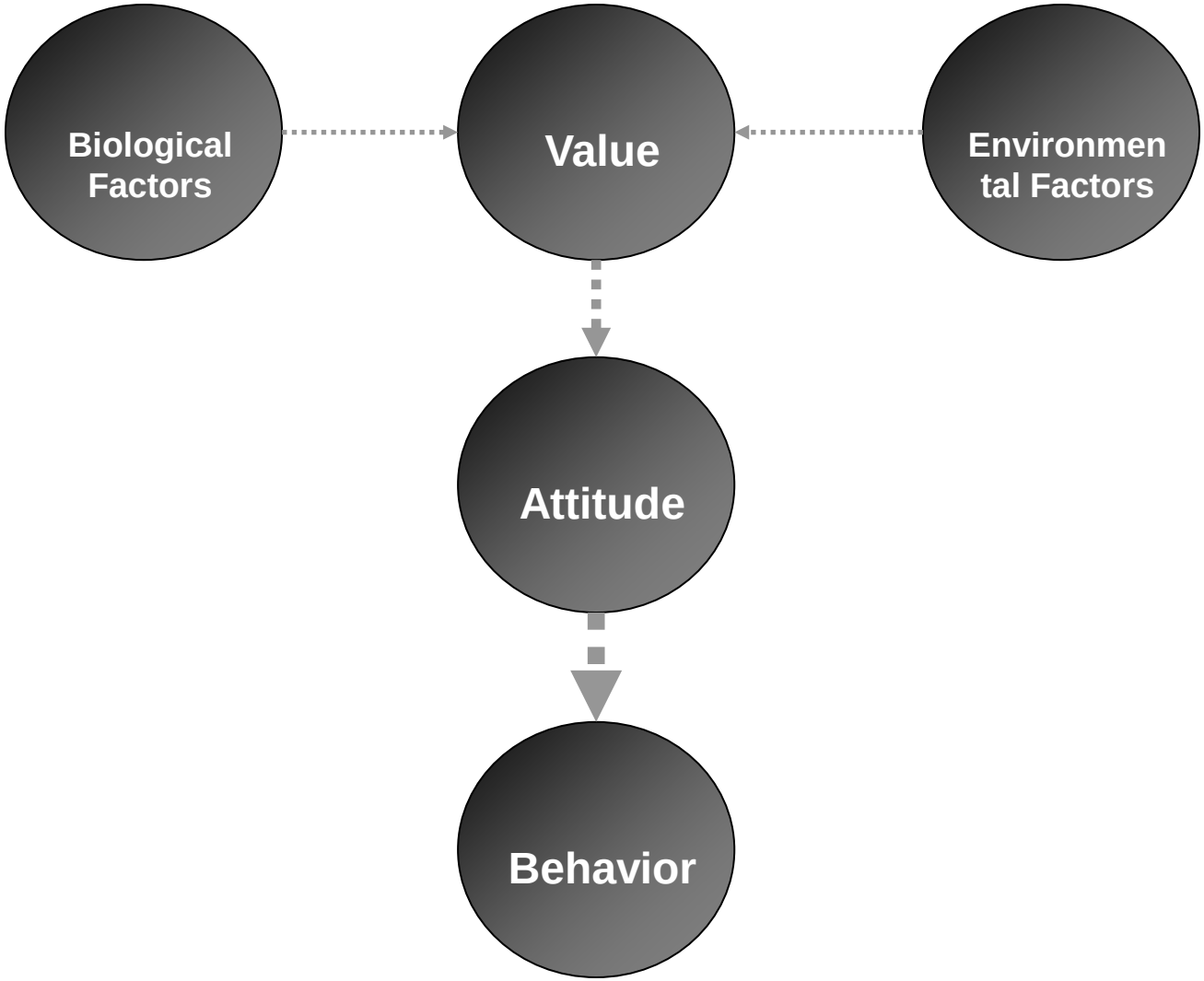
- **Attitudes – learned, global evaluations of a person, object, place, or issue that influence thought and action**
- **Values – Principles or standards about what is right and wrong one uses to make choices**

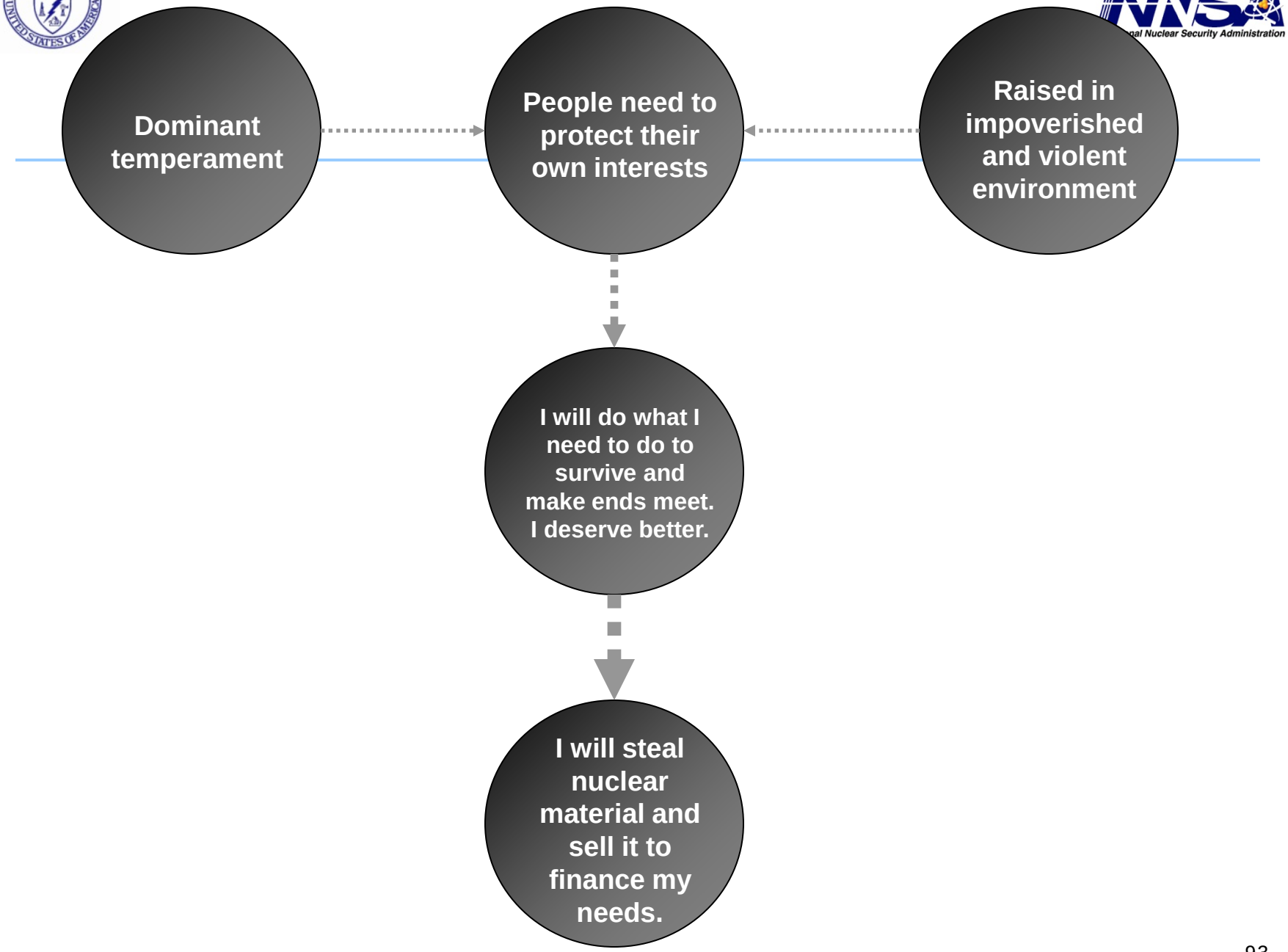
Problematic Worker Attitudes

- That's not my job
- I’m not part of the problem
- The other department should have taken care of it
- I have new responsibilities now so I can't do it
- It won't work
- It can't be done
- Because I don't make more, I'm only giving a partial effort
- I just doing this for the money until something better comes along
- My perception is different than the company’s, so I’ll do things my way
- I am considered worthless, so I’ll live up to that expectation
- There is too much change
- I have no incentives to do a good job, so why do a good job
- I have no growth possibilities, so I will not give my best
- I can't advance because of a political environment, so why try hard at work
- I don't get any respect, so I don’t give respect

Things to Know about Values

- Values generally influence attitudes and behavior
- Generally determined through biological factors (e.g., temperament) and environmental influences (e.g., national culture, parents, teachers, friends)
- Values are relatively stable and enduring
- If we know an individual's values, we are better able to predict a behavior in a particular situation


Biological Factors
Value
Environmental Factors
Attitude
Behavior


Dominant temperament
People need to protect their own interests
Raised in impoverished and violent environment
I will do what I need to do to survive and make ends meet. I deserve better.
I will steal nuclear material and sell it to finance my needs.

Working with Individual Variables

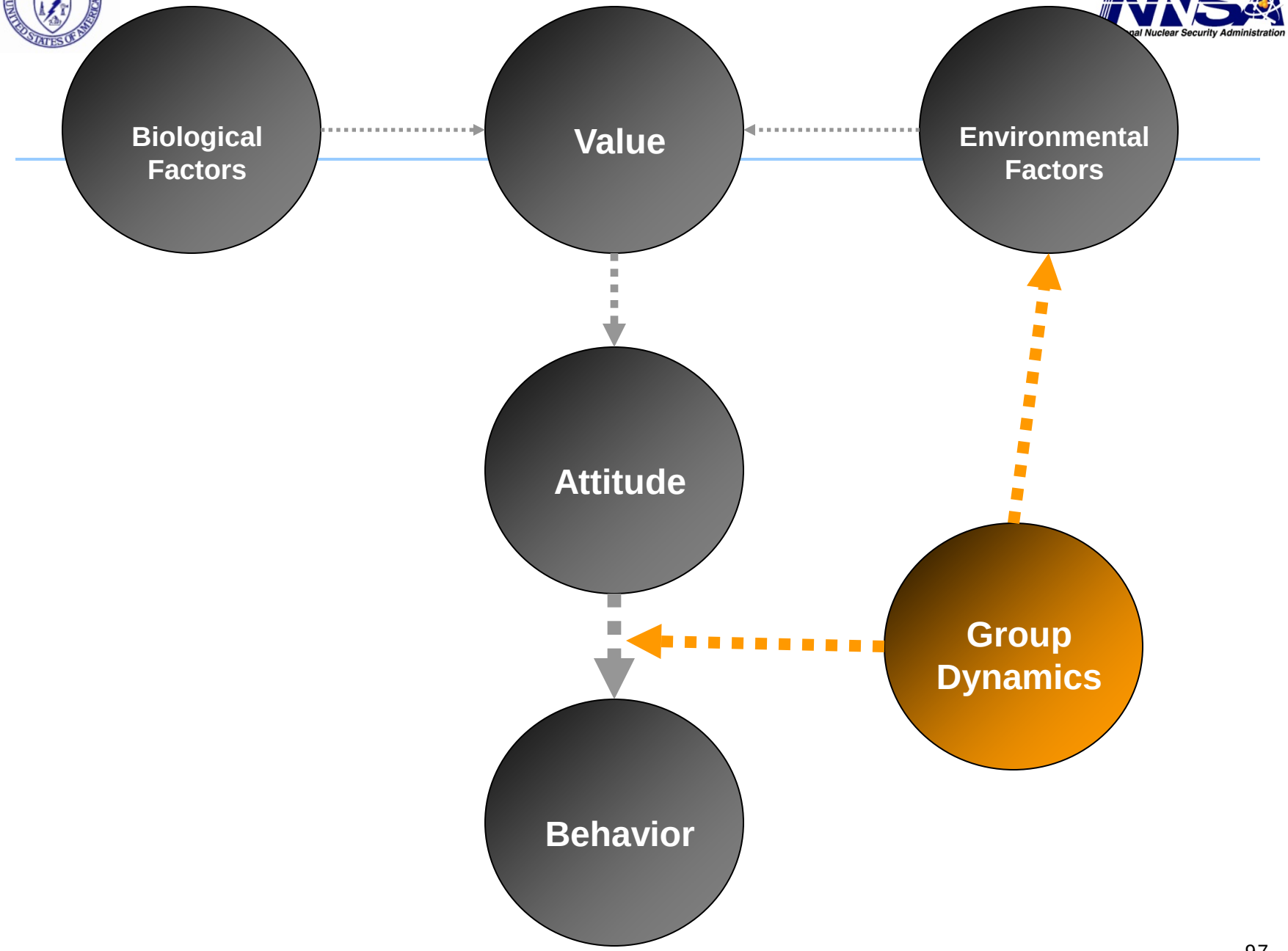
- Attitudes and values should be assessed prior to placing someone in a position of trust, but also periodically thereafter
- Creating a positive peer culture will do more to positively impact individual variables than trying to take a top-down approach (Group Dynamic)
- This being said, the leadership of any organization sets the tone for the culture (Group Dynamic)

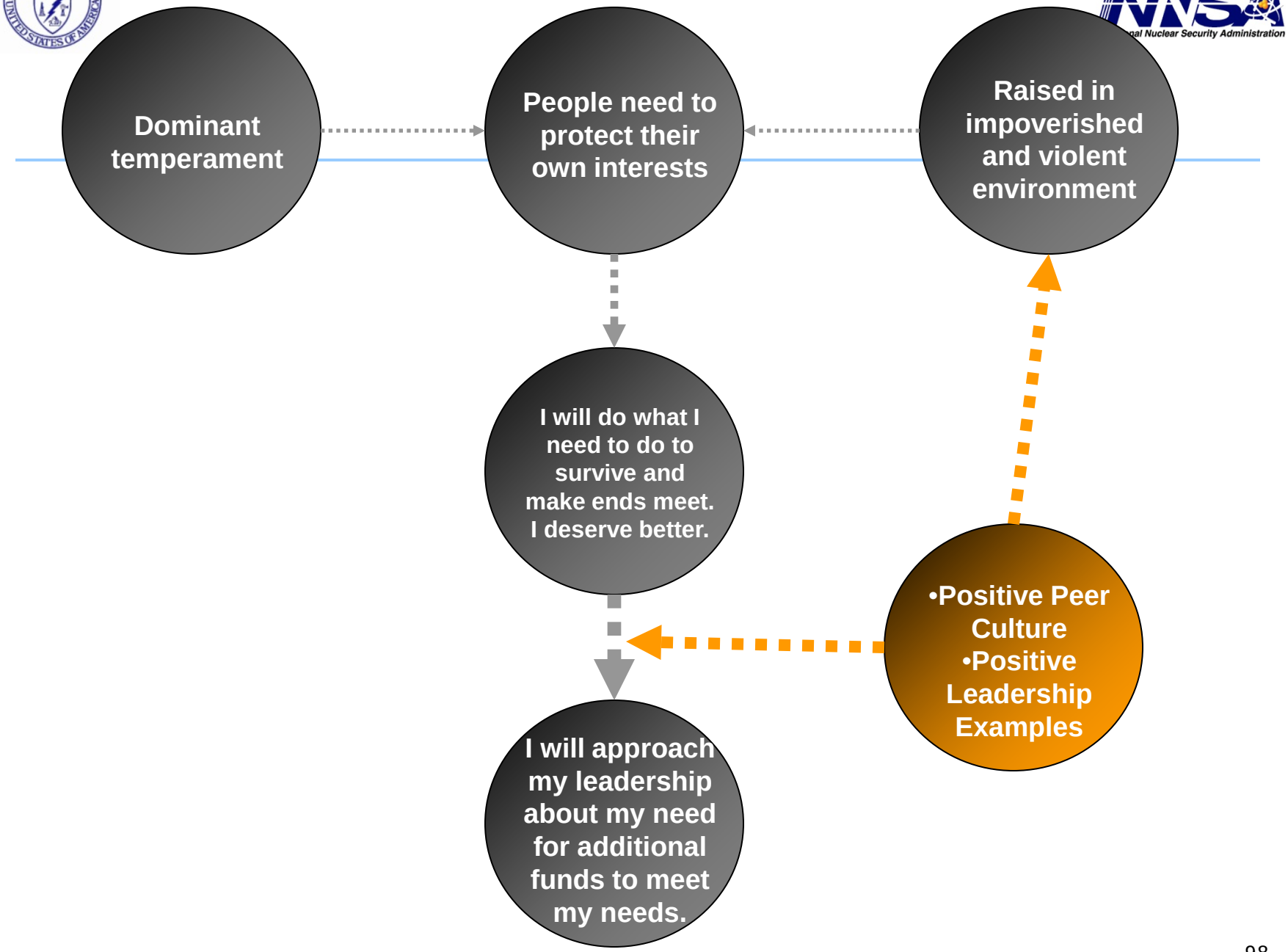
Group Variables

- Social influence – how people affect the thoughts, feelings, and behaviors of others
- Group dynamics – how people in groups tend to interact, influence each other, and share a common identity
- Culture – The predominating attitudes and behavior that characterize the functioning of a group or organization

"YOU become the average sum of the five people with whom you associate with."

Jim Rohn, American Entrepreneur
and
Best-Selling Author


Biological Factors
Value
Environmental Factors
Attitude
Group Dynamics
Behavior


Dominant temperament
People need to protect their own interests
Raised in impoverished and violent environment
I will do what I need to do to survive and make ends meet. I deserve better.
•Positive Peer Culture
•Positive Leadership Examples
I will approach my leadership about my need for additional funds to meet my needs.

Problematic Attitudes Caused by Group Dynamics

- **Social Influences –** ***"I should mind my own business and not get involved."***
- **Transfer of Responsibility –** ***"Someone else will report it. It's not my job. His supervisor should report it."***
- **Fear of Reaction –** ***"If I report it, they will either ignore it or blow it out of proportion."***
- **Conflict and Confidentiality –** ***"If people find out that I reported information, no one will trust me and the working environment will be tense."***
- **Disbelief –** ***"I can't believe that she would do something like that. I've worked with her for years, and she's as loyal as you and I."***
- **Fear of Being Paranoid –** ***"I'm being paranoid – there's nothing wrong with him. I must be overreacting, and my paranoia will do nothing but get him into trouble."***
- **Magical Thinking –** ***"If I ignore her aberrant behaviors nothing bad will happen, I will not have to deal with potential conflict, and I will not risk losing a valued employee."***

Problematic Work Culture

- Each employee only performs a “fixed job”
- Each employee is expected to perform up to minimum standards
- Pay is based on minimum performance
- Peer pressure keeps new employees from performing above minimum standards and taking initiative that goes beyond basic job requirements
- Supervisors have given up on trying to motivate employees to do anything more than what is required, having difficulty even doing this most of the time
- Leadership philosophy is based on trying to impose control

Positive Attitudes

Social Responsibility – *"I should get involved."*
Taking Responsibility – *"I will report it. It's my job to let someone know."*
Open to Reporting – *"If I report it, they will take it seriously."*
Cultural Support – *"My coworkers and supervisors understand the need to report concerns. I'm confident that my report will remain confidential."*
Threat is Real – *"I do not know if she is an insider threat; however, the threat is real and she fits the profile, so I must take action."*
Self Validation – *"I have the impression and evidence that he is exhibiting aberrant behavior. I cannot allow myself to hope that I am wrong. The potential impact if I am right but do not report is too high."*
Rational Thinking – *"If I do not report her aberrant behaviors I may avoid the stress of potential conflict, but I take the risk of allowing a malicious insider to damage the organization and national security."*

Positive Peer Culture

- Employees work on teams, where teams have a “fixed job” rather than the members
- Each team member is given the training necessary to do most, if not all of the other jobs on the team
- Pay reflects mastery of skills
- Team has received assurances by management that should there be an economic downturn that requires downsizing, they will be put to work somewhere, as they are valued
- Team members have been given the “big picture” and understand their role and importance to the overall vision of the organization
- Leadership philosophy is based on trying to elicit commitment

How NSC Mitigates Malicious Insider Behavior

Mitigating the Relationship Between Attitudes and Behaviors

4 Mediators between Attitudes and Behaviors

- **Susceptibility to being caught**
- **Severity of consequences**
- **Hardship/benefit ratio**
- **Barriers to taking malicious actions**

A strong NSC increases susceptibility, severity, hardship/benefit ratio, and barriers, making malicious insider behavior less likely

Susceptibility to Being Caught

Malicious Insider
How ***likely*** one thinks a bad outcome is if behavior persists and one is caught
Example: Getting caught for theft of nuclear material
As susceptibility increases, the likelihood of malicious behavior decreases

Severity of Consequences

Malicious Insider

The **degree of unpleasantness** associated with the consequence if the behavior persists and one is caught

Example: Going to prison for theft of nuclear material

As severity increases, the likelihood of malicious behavior decreases

Hardship / Benefit Ratio

Malicious Insider

The **ratio of negative to positive consequences** if the behavior persists and one is caught

Example: Going to prison for theft of nuclear material versus obtaining funds to purchase a vehicle

As the hardship to benefit ratio increases, the likelihood of malicious behavior decreases

Barriers to Taking Malicious Actions

- The **significance of obstacles** to engaging in the behavior
  - Psychological *(e.g., self-worth)*
  - Financial *(e.g., no means to get material to the buyer)*
  - Temporal *(e.g., not enough time alone in the vault to access nuclear material*)
  - Physical *(e.g., alarms are maintained and responded to without fail)*
  - Interpersonal (e.g., associates at work are diligent with regard to NSC)
- As the number of barriers increases, the likelihood of malicious behavior decreases

Example: Not likely to Steal Nuclear Material

- Employee thinks that he will get caught if he continues to divert small amounts of nuclear material from vault (susceptibility).
- Employee believes that she will be sent to prison for life if he is caught (severity).
- Employee believes getting caught and being sent to prison for life far outweigh the benefit of obtaining cash for nuclear material (hardship/benefit).
- Employee's coworkers are vigilant and there is a strong NSC in his organization (barrier)

Lessons Learned From U.S. Human Reliability Program

- Key to success is integration of security, management, coworker, psychological and medical data
- All employees with “access” should be part of HRP program
- HRP decision making process should be independent from political or management pressures
- All HRP staff need regular education regarding the reality of the threat and the importance of their role
- HRP program needs to have access to resources to assist employees at risk
- Temporary removal should be exercised regularly and truly have no impact on pay/promotion potential