LA-UR-19-22069
Approved for public release; distribution is unlimited.

Title: Overview of Tools for Insider Threat: Analysis and Mitigation

Author(s): Scherer, Carolynn P.
Ruggiero, Christy E.

Intended for: Institute of Nuclear Material Management (INMM) Just Trust Me Workshop, 2019-03-12/2019-03-13 (Albuquerque, New Mexico, United States)

Issued: 2019-04-10 (rev.1)

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Overview of Tools for Insider Threat: Analysis and Mitigation

LA-UR-19-22069

INMM Just Trust Me Workshop

March 12-13, 2019

Christy Ruggiero

Carolynn Scherer

3/12/2019

Managed by Triad National Security, LLC for the U.S. Department of Energy's NNSA

Overview

Helping INS develop an Insider Threat Mitigation Program

Talk Outline:

- INS Mission
- Insider Threat Mitigation Program (ITMP) Components and Roadmap
- INS ITMP tool box:
  - Broad Resources, Guidance, Tools
  - Insider Threats in Nuclear Security Analyses
    - Design Basis Threat (DBT) & Vital Area Identification (VAI)
    - Risk Assessment
    - Vulnerability Assessment (VA)
- People & Culture Tools

Mission Space

DOE/NNSA →

Office of Global Material Security (GMS) →

International Nuclear Security (INS):

Mission is to "lead U.S. international efforts to prevent theft and sabotage of nuclear materials and facilities worldwide."

How can the U.S. help countries improve their Nuclear Security?

INS→

Insider Threat Mitigation Working Group (ITMWG)

Help INS improve nuclear security capabilities that protect nuclear materials and facilities against theft, sabotage, unauthorized access while in use, storage, or transit by addressing INSIDER THREATS.

How can we help improve their <u>Insider Threat Mitigation Programs?</u>

International Nuclear Security

Partnering for a Secure World

The consequences of nuclear terrorism represent a grave threat to national and international security. To help address the risk of nuclear material theft or sabotage of nuclear facilities, the Office of International Nuclear Security (INS), under the U.S. Department of Energy's National Nuclear Security Administration (DOE/NNSA), works with partner countries and multilateral organizations to enhance nuclear security worldwide.

Mitigating Threats to Nuclear Facilities

Maintaining an effective domestic nuclear security regime that responds to changing threats and risks is the responsibility of all States. INS partners with a range of nuclear stakeholders including international organizations, government agencies, competent authorities, operators, nuclear facility managers and staff, and guard force organizations to help build or improve nuclear security capabilities. Through these interactions, INS shares knowledge to improve capability and capacity to address the full spectrum of threats to nuclear security.

Strengthening Global Nuclear Security Practices

INS has more than 20 years of experience working with international partners to enhance nuclear security and can draw upon the extensive technical capabilities of the U.S. DOE National Laboratories. INS provides the expertise, tools, and systematic approach necessary to improve and sustain effective nuclear security. INS achieves this objective by:

- Providing technical support for the IAEA efforts to improve nuclear security worldwide through the development of guidelines and training, conduct of training activities, and International Physical Protection Advisory Service (IPPAS) missions
- Coordinating with partner organizations to develop and foster the adoption of effective nuclear security technical and performance standards and guidelines for material in use, storage, and transport

Nuclear Security Engagement and Training

INS works with partner countries to implement nuclear security training and conduct best practice and technical exchanges. These activities facilitate engagement between technical professionals on topics including:

- Nuclear Security Principles
- Physical Protection

- Response Force Practices
- Nuclear Material Accounting and Control
- Fixed Site Security
- Transportation Security
- Cyber Security Impacts on Nuclear Security
- Nuclear Security Culture
- Mitigating the Insider Threat

Working with training centers and nuclear security support centers, INS fosters sustainable indigenous training programs through support for curriculum development and instructor training to help expand nuclear security training capacity internationally.

Nuclear Security Enhancements and Infrastructure Support

INS works with international partners to support the design and implementation of nuclear security systems at all types of nuclear facilities. In addition, INS engages with partners to implement nuclear security infrastructure at training centers, and enhance programs related to nuclear security culture, regulatory development, and associated inspections.

Email: INSInfo@nnsa.doe.gov
Website: https://nnsa.energy.gov/

National Nuclear Security Administration

INS Partnering for a Secure World International Nuclear Security

ITMWG Objective: Improve Tool Box

We need a unified INS approach for engagement with other countries on Insider Threat Mitigation:

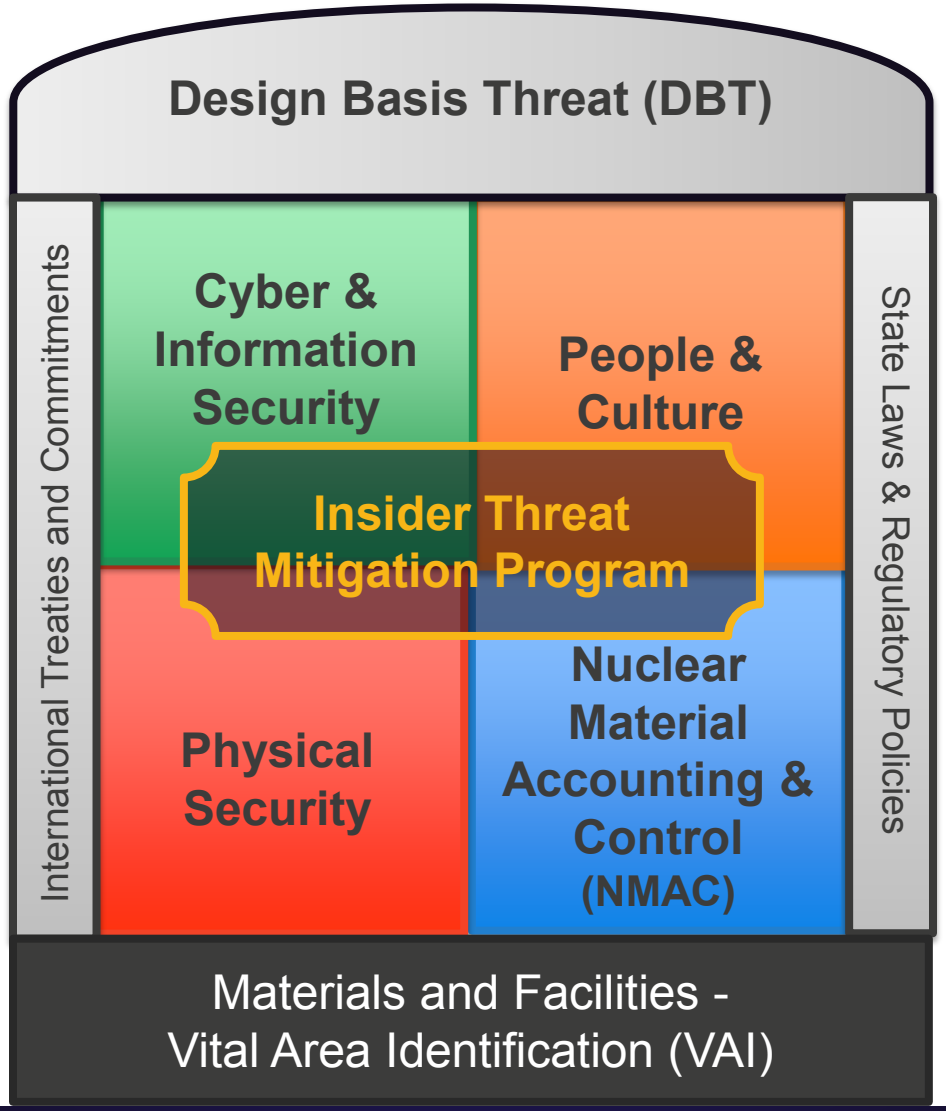
- Standards & Best Practices
- Methodologies & Guides
- Tools, Resources, Codes
- Examples, Procedures, Checklists, Other help

Starting Questions for Toolbox:

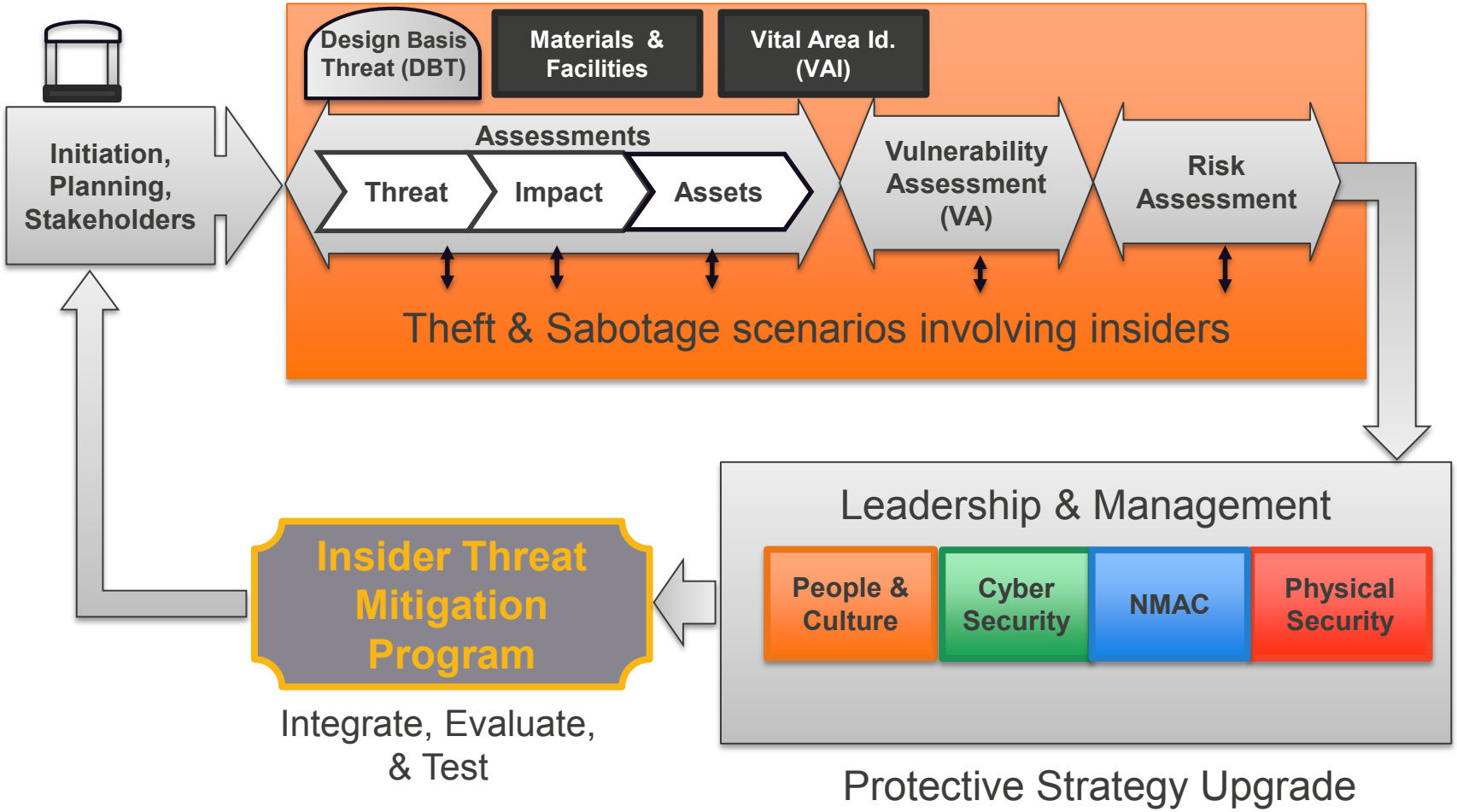
- ***What are the components*** *of a complete insider threat mitigation program?*
- *What tools/resources/methods can be used to* ***initiate, support, operate, assess, and sustain*** *an insider threat mitigation program?*
- *How well do these tools address current and emerging insider threats?*
- *How could the tools be improved?*

Help us compile & evaluate resources, tools, best practices….

Insider Threat Program Components



Basic Insider Program Roadmap

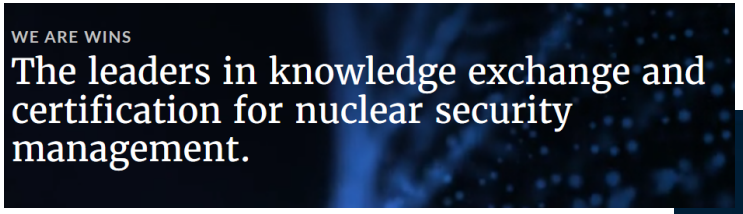


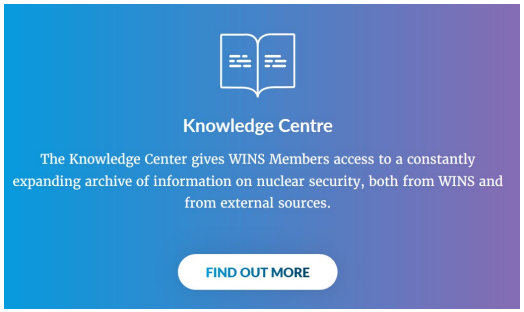
Insider Threat Mitigation Program: Guidance & Resources

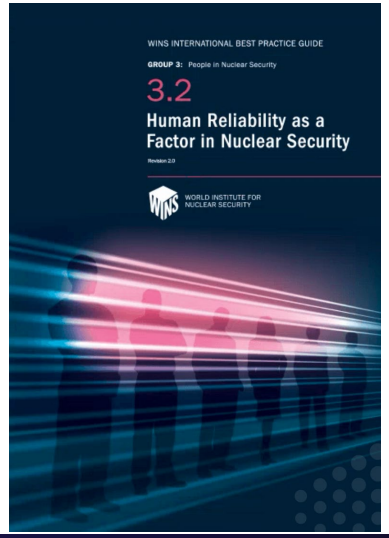
Foundations: WINS

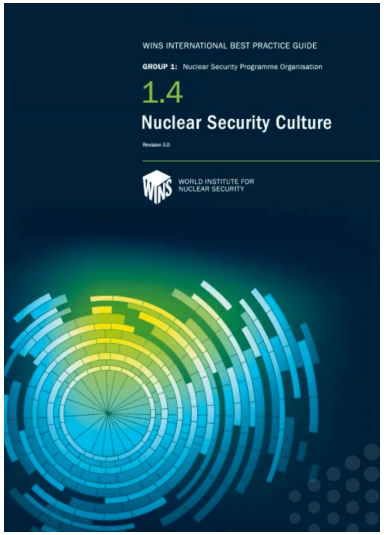
World Institute for Nuclear Security (WINS)

"The World Institute for Nuclear Security operates as an independent, not for profit, international non-governmental organisation, whose Vision is to help ensure that "all nuclear and other radiological materials and facilities are effectively secured by demonstrably competent professionals applying best practice to achieve operational excellence".

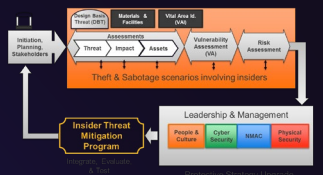








Foundations: IAEA

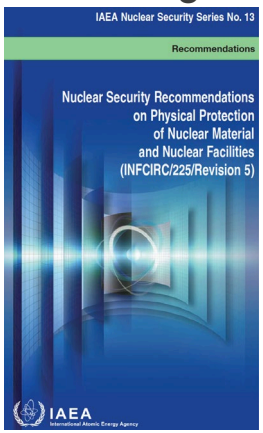


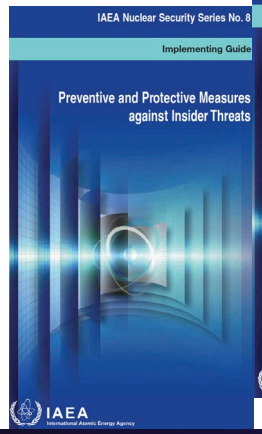
Nuclear Security Series (NSS):

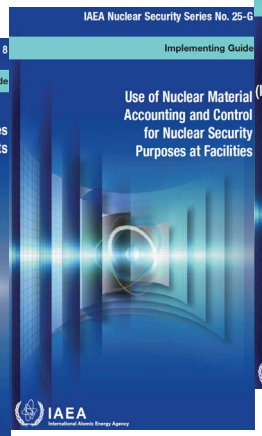
- 13-R: “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities” (INFCIRC/225/Revision 5)
- 8-G: “Preventive and Protective Measures against Insider Threats”
- 25-G: “Use of Nuc. Material Accounting & Control for Nuc. Security Purposes at a Facility”
- 27-G: “Implementing Guide, Physical Protection of Nuclear Material and Nuclear Facilities” (Implementation of INFCIRC/225/Revision 5)
- 28-T: “Self-assessment of Nuclear Security Culture in Facilities and Activities”

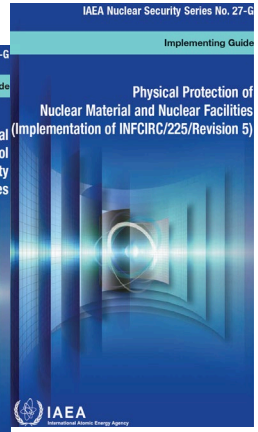
Other:

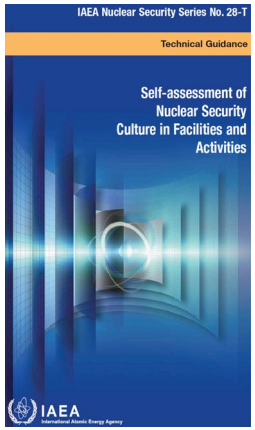
- International Physical Protection Advisory Service (IPPAS)
- Open Learning Management System (LMS): Insider threat, National and Regional course offerings and e-learning modules



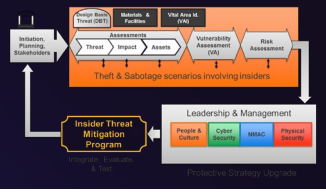








Foundations: U.S. – IAEA: INFCIRC/908



- **INFCIRC/908**
  - Request countries to become signatory
- International Workshop in Brussels, Belgium March 12-14, 2019

IAEA 60 Years
Atoms for Peace and Development

Information Circular

INFCIRC/908
Date: 9 January 2017

General Distribution
Original: English

Communication dated 22 December 2016 received from the Permanent Mission of the United States of America concerning a Joint Statement on Mitigating Insider Threats

Joint Statement on Mitigating Insider Threats

Insider Threat Program Developments: U.S.

U.S. Classified Network Security-Basic requirements:

- **Executive Order (EO) 13587:** Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 2011)
- **White House Memorandum: National Insider Threat Policy and Minimum Standards** for executive Branch Insider Threat Programs (Nov. 2012)
- **White House Memorandum:** Compliance with President's Insider Threat Policy (July 2013)

The White House
Office of the Press Secretary

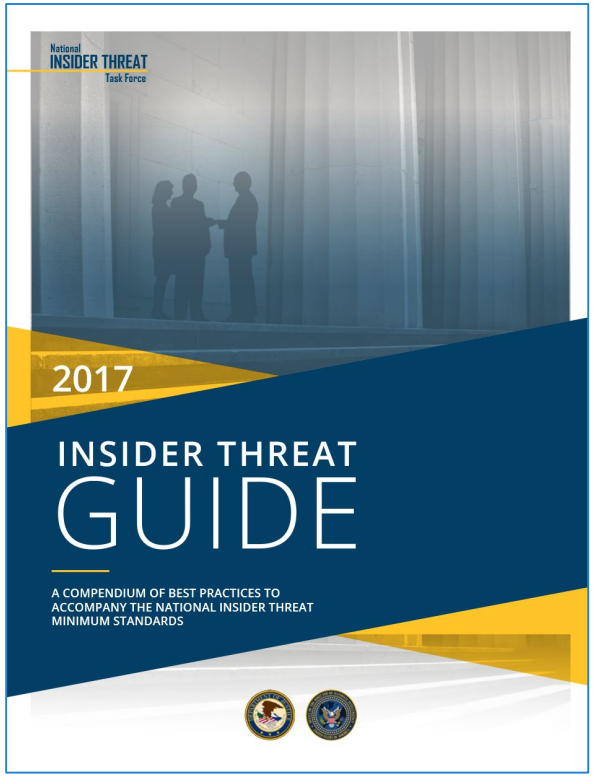
For Immediate Release October 07, 2011

Executive Order 13587 -- Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

U.S. E.O. to U.S. Task Force

From E.O. 13587 → National Insider Threat Task Force (NITTF)

- ***Insider Threat Guide (NITTF-2017)***
  "A Compendium of best practices to accompany the nation insider threat minimum standards"
- ***NITTF website***
  - Similar to WINS/IAEA best practices, but for U.S. classified information protection.
  - Top level focused.
  - Lots of material including policy templates, training aids, reference documents, **large tool kit!**



DOE Order 470.5 → *Insider Threat Program*

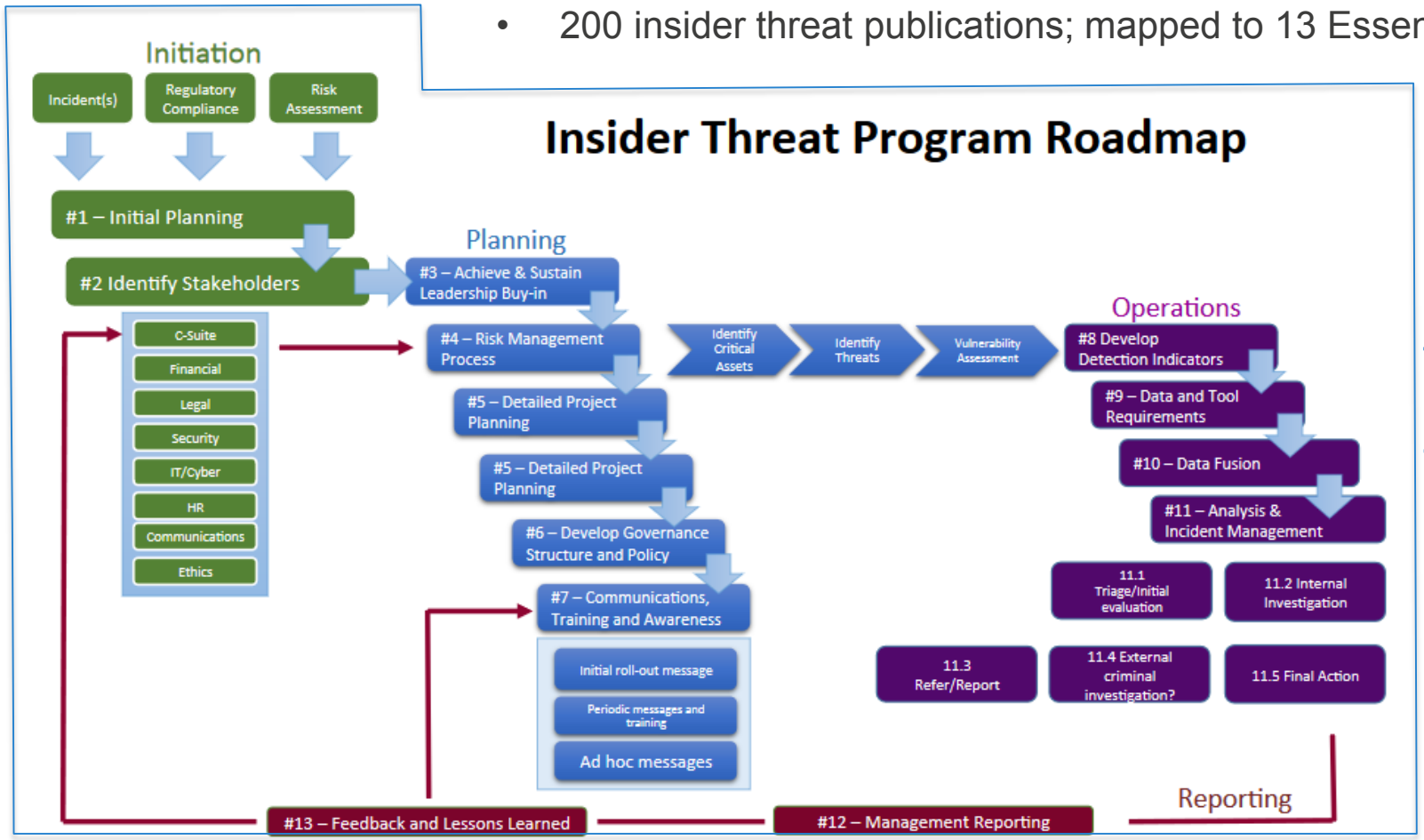
"To establish responsibilities and requirements for the Department of Energy (DOE) Insider Threat Program (ITP) to deter, detect, and mitigate insider threat actions by Federal and contractor employees in accordance with the requirements of Executive Order 13587…….and other government-wide and DOE requirements."

Intelligence and National Security Alliance (INSA)

INSA Roadmap:

Our group set out to develop a resource that provides the essential elements required to initiate an ITMP…"

- 13 Essential Elements that follow a timeline
- 200 insider threat publications; mapped to 13 Essential Elements



Resource for any organization that is creating or maturing an ITMP

Center for Development of Security Excellence (CDSE)

- Provides security education and training for the DoD and industry under the National Industrial Security Program (NISP).
- Similar to WINS, but for security for Industry-Department of Defense interface programs
- A lot of insider threat resources—
  - ✓ Education
  - ✓ Training
  - ✓ Certification
  - ✓ Checklists & Job aids
  - ✓ ToolKit

Defense Security Services: www.cdse.edu

Insider Threat Indicators & Monitoring Activities-CDSE

People & Culture

Insider Threat Indicators in User Activity Monitoring

User Activity

Performance

Foreign Travel/Contacts

Financial Issues

Conduct

Addictions

Kinetic Violence

The FBI Top 21 Concerning Behaviors

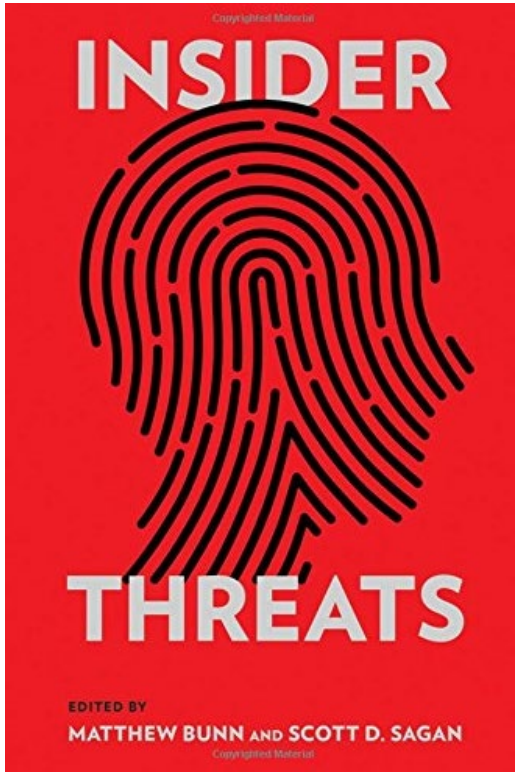
1. Mental health
2. Interpersonal interactions
3. Communicating intent to harm someone
4. Quality of thinking or communication
5. Work performance
6. School performance
7. Threats/confrontations
8. Anger
9. Physical aggression
10. Risk-taking
11. Firearm behavior
12. Violent media usage
13. Weight/eating
14. Drug abuse
15. Impulsivity
16. Alcohol abuse
17. Physical health
18. Other (e.g. idolizing criminals)
19. Sexual behavior
20. Quality of sleep
21. Hygiene/appearance

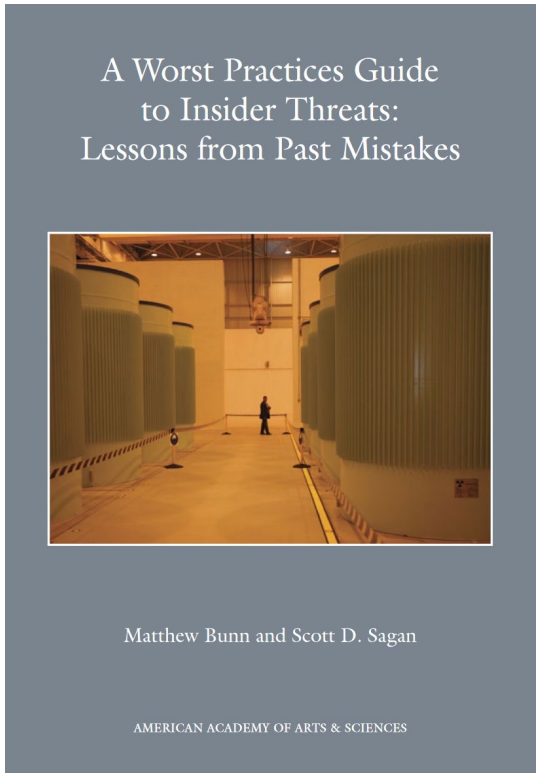
https://www.cdse.edu/documents/cdse/InsiderThreatIndicatorsUAM.pdf;
https://www.cdse.edu/documents/cdse/potential-risk-indicators-kinetic-violence-jobaid.pdf

Academic

- Bunn & Sagan: A Worst Practices Guide to Insider Threats
- Bunn & Sagan: Insider Threats (2017)

There are many others…most not specific to nuclear



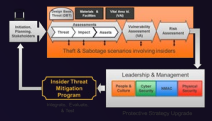


Commercial

- **Ernst & Young (E&Y) Managing Insider Threat**
  - Big company, big data analytics branch
  - Experience in fraud & asset protection
  - 8 steps to building program
  - Maturity Model
- **Tanager-Insider Threat Program**
  - Full spectrum services: implementation, training, tool selection, analysis, consulting, technology

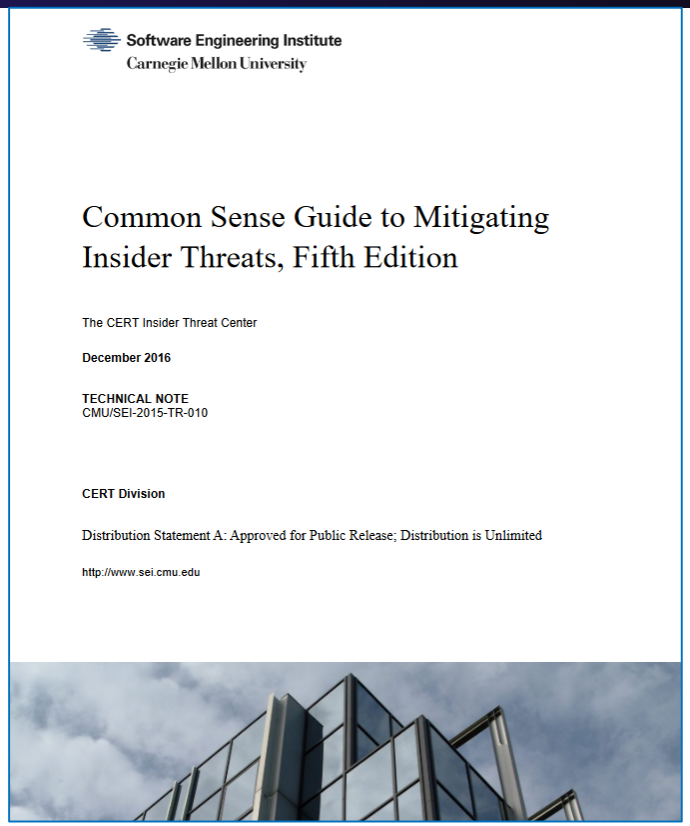
There are many others…most not specific to nuclear, but all usable/adaptable

Develop INS Insider Threat Tool Box



Optimize elements for INS toolbox for Insider Threat Mitigation Program for international engagement using growing body of related standards and best practices.

1. Leverage elements from cyber & information security best practices, guides & resources
2. Coordinate and combine with components from WINS
3. Align with emerging consensus and standards
4. Harmonize into INS terminology/program guidance



Software Engineering Institute
Carnegie Mellon University

Common Sense Guide to Mitigating Insider Threats, Fifth Edition

The CERT Insider Threat Center

December 2016

TECHNICAL NOTE
CMU/SEI-2015-TR-010

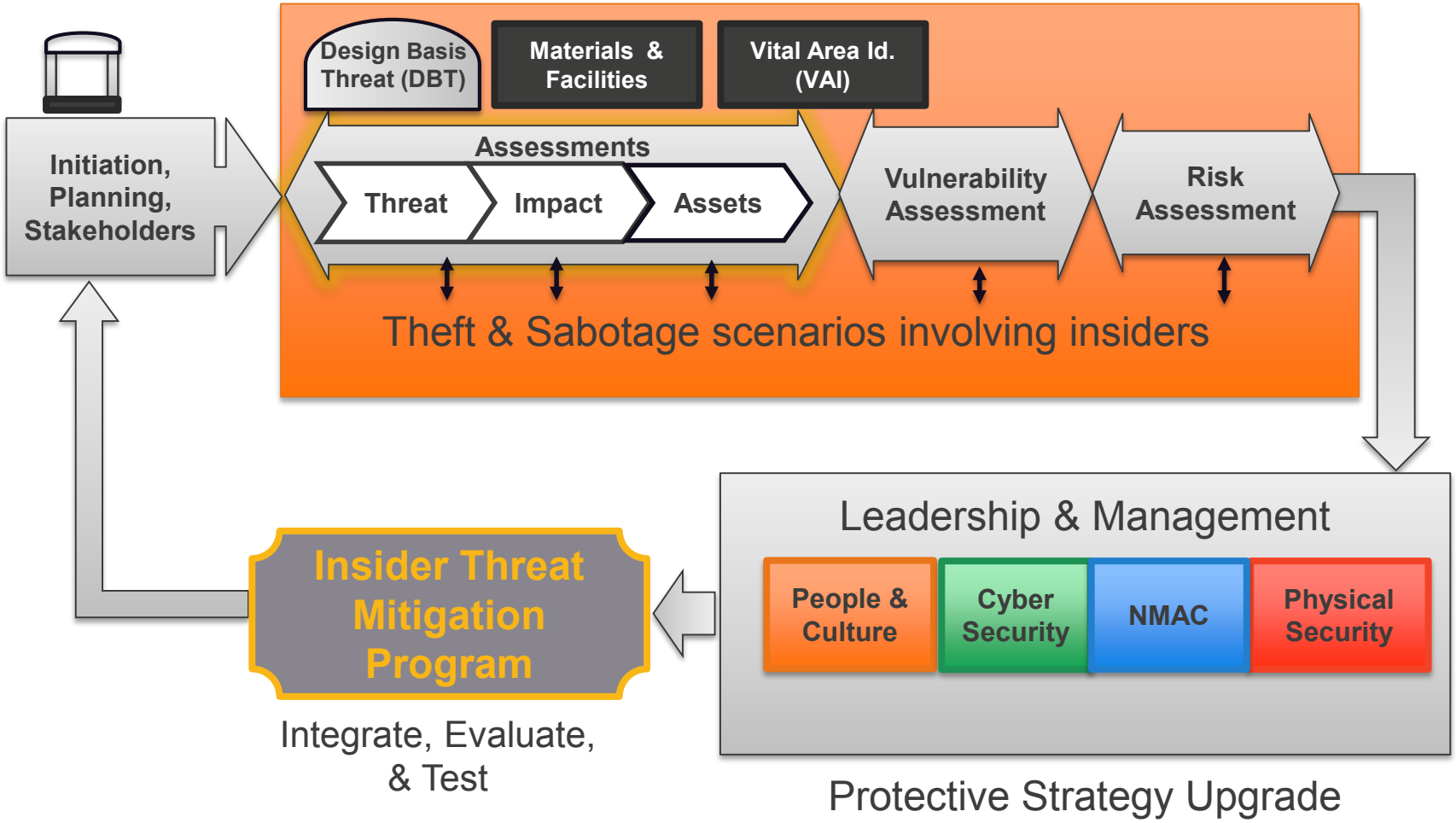
CERT Division

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

http://www.sei.cmu.edu

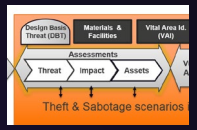
- 175 Pages
- 20 Practices, each with protective measures, challenges, case studies
- Practices mapped to Standards
- Practices mapped to groups within organization
- Checklists of easy high win solutions

INS – Roadmap for ITMP



Design Basis Threat & Vital Area Identification

Foundations: DBT Threat Assessment



Well-established and accepted for Nuclear Threat Assessment for theft of category 1 nuclear material and sabotage with high radiological consequences.

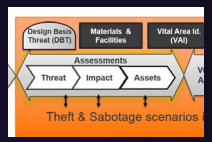
Threat assessment is an "evaluation of the threats – based on available intelligence, law enforcement and open source information-that describes the motivations, intentions and capabilities of these threats"

"A DBT is a description of the attributes and characteristics of potential insider and outsider adversaries who might attempt a malicious act, such as unauthorized removal or sabotage against which a physical protection system for nuclear or other radioactive material or associated facilities is designed and evaluated."

"The design basis threat is a regulatory tool for planning, designing, and evaluating a physical protection system."

DBT defines what the threats are…

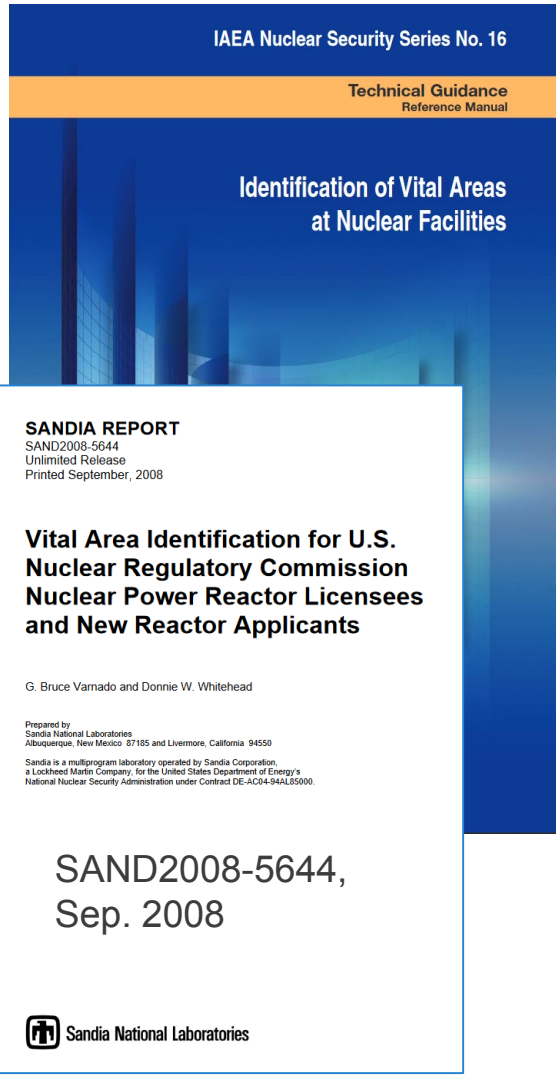
Foundations: Vital Area Identification (VAI)



Vital Area: An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences (HRC)

Vital Area Identification (VAI) is the process of identifying the areas of a nuclear facility that must be protected to prevent malicious acts that could directly or indirectly endanger the public health and safety by exposure to radiation

DBT & VAI may not fully incorporate insider threats …


IAEA Nuclear Security Series No. 16

Technical Guidance
Reference Manual

Identification of Vital Areas at Nuclear Facilities

SANDIA REPORT
SAND2008-5644
Unlimited Release
Printed September, 2008

Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants

G. Bruce Varnado and Donnie W. Whitehead

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

SAND2008-5644, Sep. 2008

Sandia National Laboratories

DBT & VAI for Insider Threat Mitigation

Insider are different:

- More **knowledge, authority, access**
- More **TIME & OPPORTUNITY** to carry out acts.
- Different **motivation and goals**
- Different **target areas** that will not lead to "High Radiological Consequences"
- Different **desired consequences**: human/health, environment, economic consequences, or just shut down facility.

Lots of guidance & resources are being developed, but still hard for DBT/VAI to cover insider threats well.

Threat & Scenario Resources for INS ITM Toolbox

Tools to help assessment folks think like an insider:

- Provide nuclear-adapted INSIDER threat statement & full scenario examples based on actual actions/attempts ….
  - from other industries:
    - High consequence industries (e.g. chemical)
    - Industries with high level of cyber-physical integration
    - Critical infrastructure industry
  - using expanded targets:
    - Targeting multiple safety/security features
    - Outside of traditional safety analysis
    - Multiple malicious insiders
    - Multiple insider using unwitting insider
- Provide statistics that can help with for evaluating likelihood of a scenario.

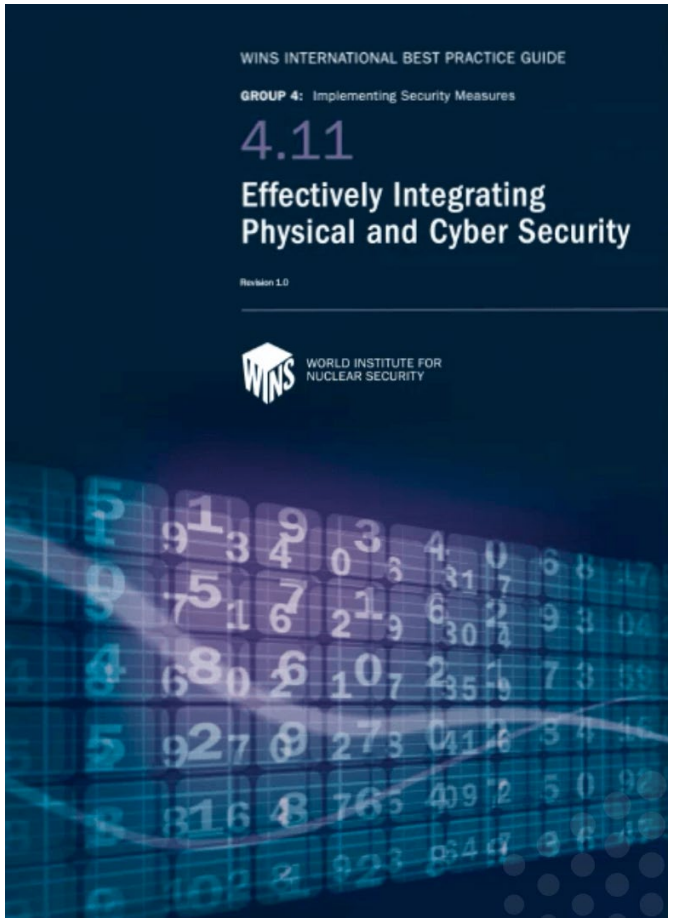
Cyber-Physical Integration resources for DBT/VAI:

Insider Threat Mitigation DBT/VAI needs better integration with Cyber security

- Joint DBT for Physical and Cyber ??
- VAI with expanded Critical Assets ??
  - ✓ Facility/Process controls--Internet of things.
  - ✓ Networked sensors/detectors/access controls
  - ✓ Cyber/physical integration targets
  - ✓ Information critical asset (Information security)
    Protected / Sensitive information

OR

- DBT combine with Cyber into a
  Probabilistic Risk Assessment?

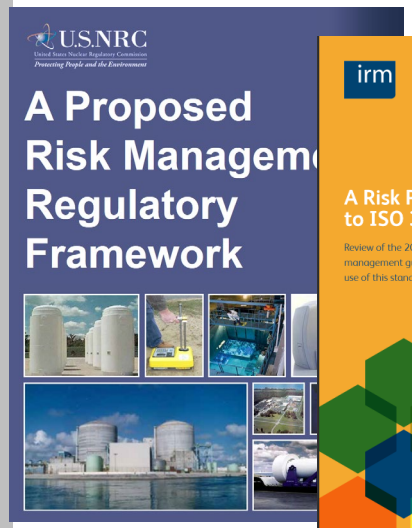


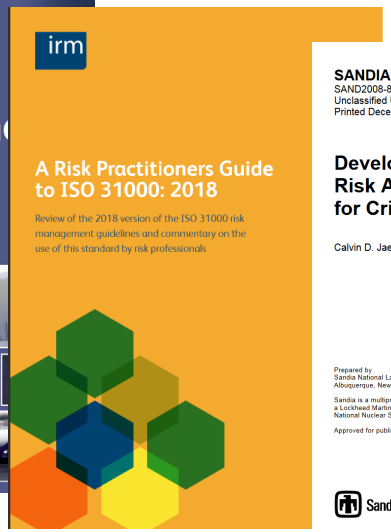
Use Risk Assessment in INS Toolbox??

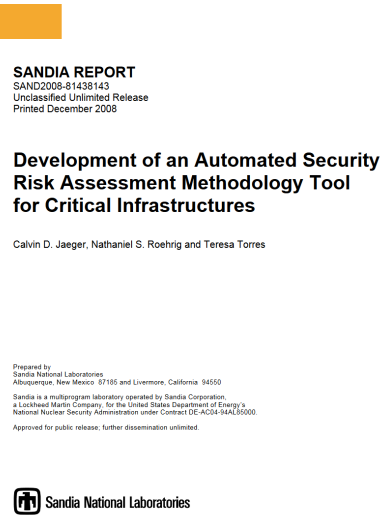
ISO 31000: 2018 Risk Management Guidelines

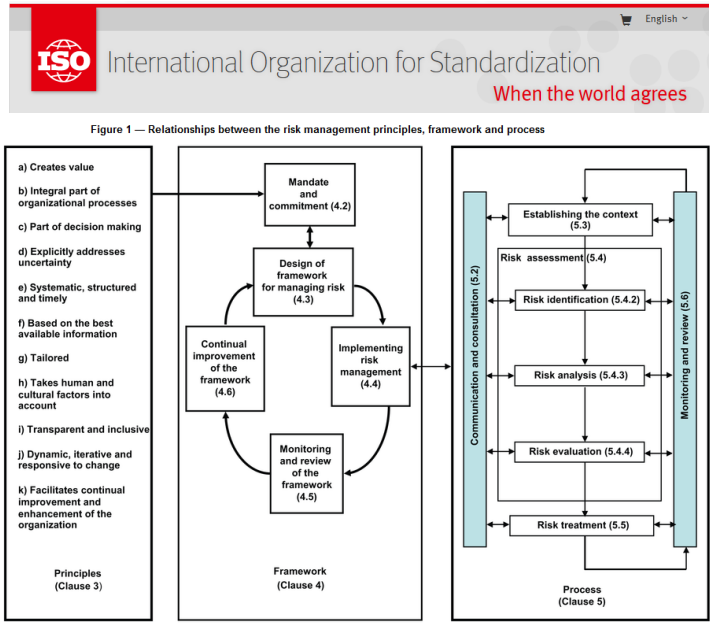
"Damage to reputation or brand, cyber crime, political risk and terrorism are some of the risks that private and public organizations of all types and sizes around the world must face with increasing frequency. The latest version of ISO 31000 has just been unveiled to help manage the uncertainty"

- Solid mature framework, professional standards, international.
- Helps prioritize resource investments.
- Many tools, both open source & commercial, that are compliant with ISO 31000.

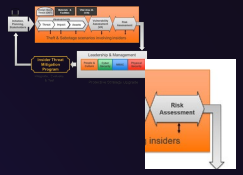








Risk Management used in Nuclear industry



Active Risk Manager
for the Nuclear Industry

SWORD
ACTIVE RISK

Active Risk Manager (ARM): The Technology Behind Leading Edge Risk Management

Successful Nuclear organizations have world-class risk management.

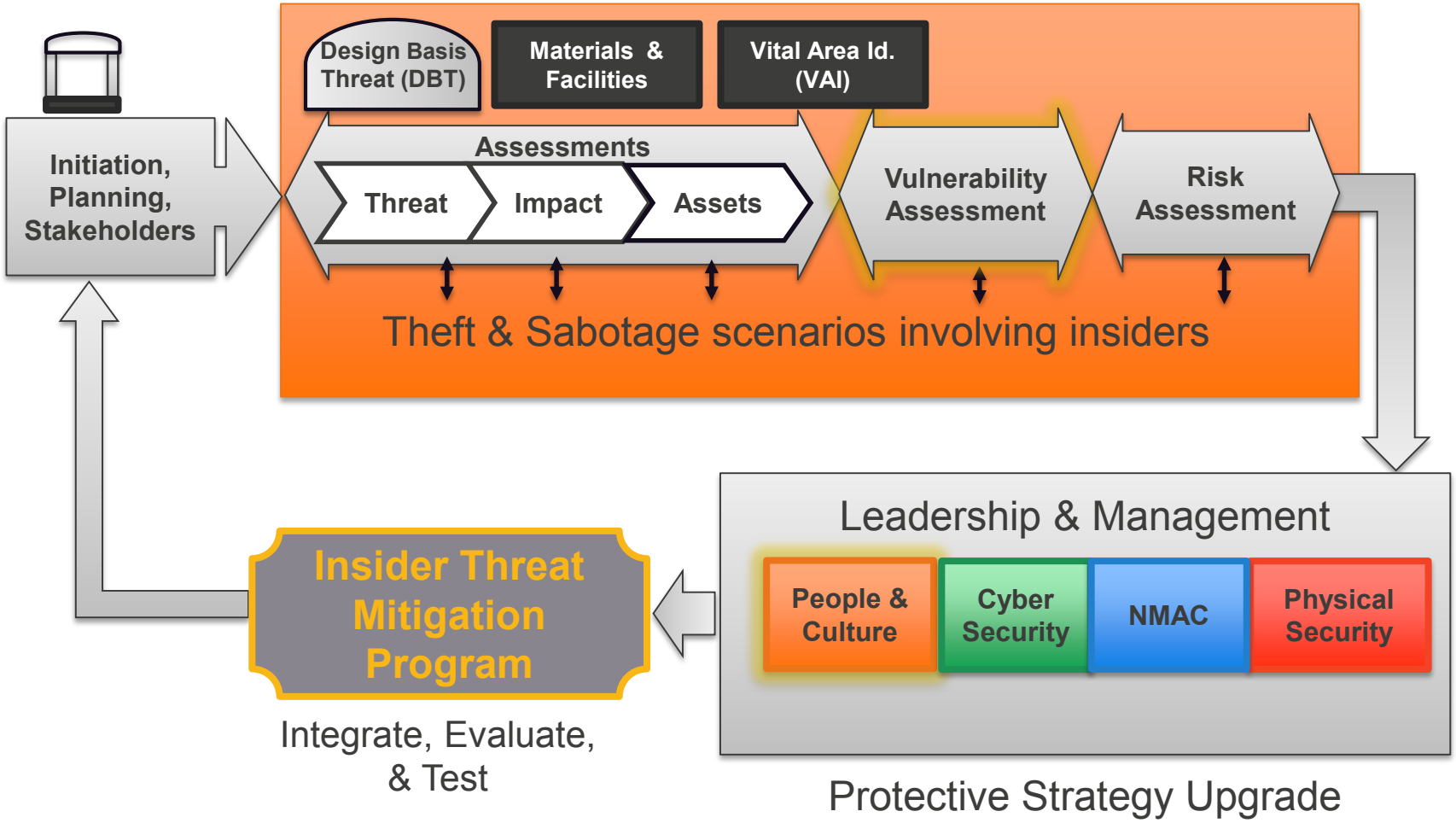
Sellafield Ltd

Sellafield Ltd is a wholly owned subsidiary of Nuclear Management Partners (NMP) a consortium of American company URS, British company AMEC and French company Areva. Sellafield Ltd is the company responsible for safely delivering decommissioning, reprocessing and nuclear waste management activities on the Sellafield nuclear site in West Cumbria, England on behalf of the Nuclear Decommissioning Authority (NDA)

"Using ARM we realised that we could cover every aspect of the work breakdown structure across the business, from the highest strategic risks to operational tasks, and we could use ARM's functionality to indicate the crucial interdependencies across the organisation."

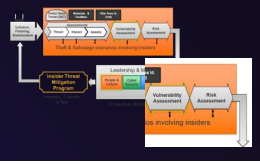
Gary Williams Risk Systems Manager Sellafield Ltd

INS Roadmap for ITMP



Vulnerability Assessment (VA)
Security Effectiveness Assessment

Foundations: INS already has VA resources



Courses/workshops:

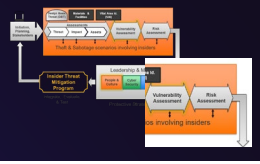
- **INS Introduction to Vulnerability Analysis**

  Vulnerability Assessment analyzes prevention, detection, delay, and response to theft, sabotage, unauthorized access, illegal transfer, or other malicious acts with radioactive and nuclear material and associated facilities

- **INS Technical Introduction to Cybersecurity at Nuclear and Radiological Facilities**

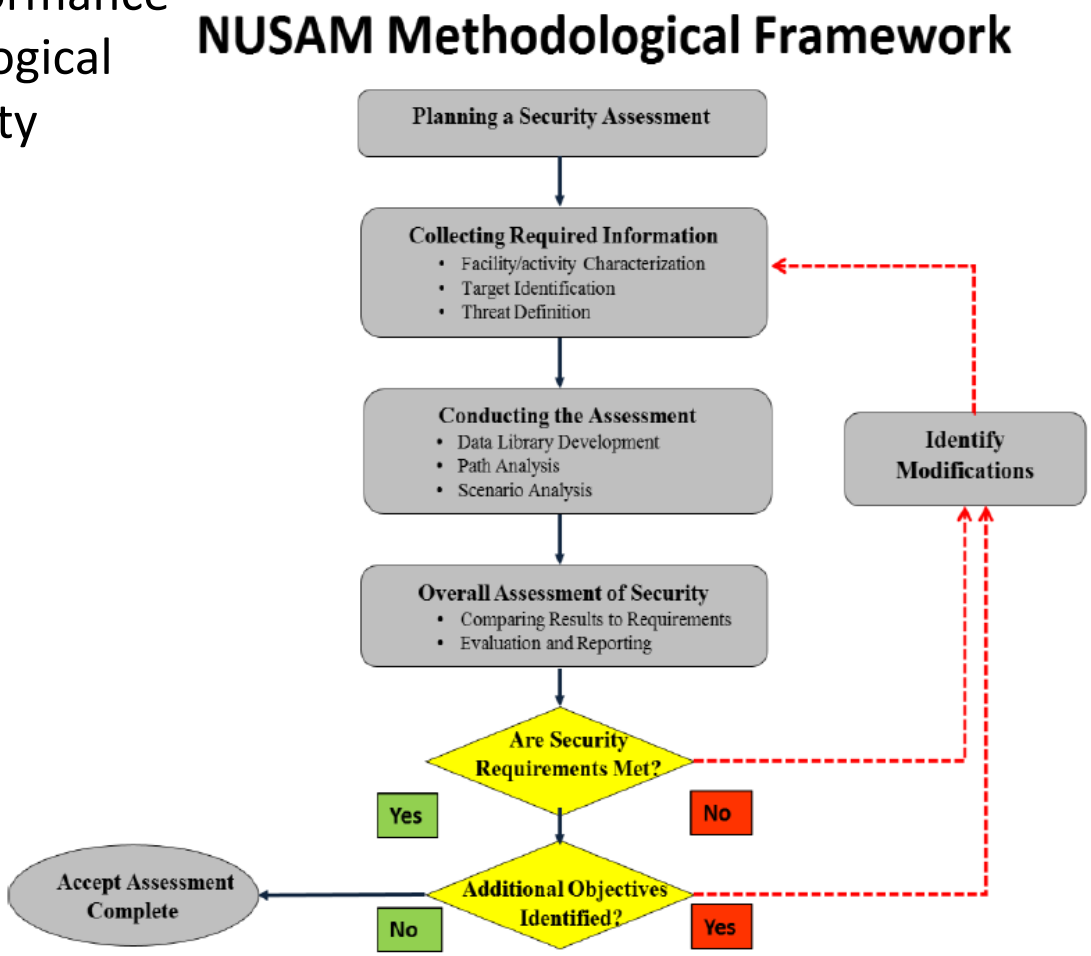
  Course content examines: cybersecurity guidance, policy, programs, and plans; differences between nuclear cybersecurity and traditional information technology security; components of industrial control systems; cybersecurity threats and risks; employee roles and training; and methods to mitigate risk.

IAEA has Guidance & Resources - NUSAM



Nuclear Security Assessment Methodology (NUSAM):

IAEA project to develop a performance based risk-informed methodological framework for assessing security effectiveness

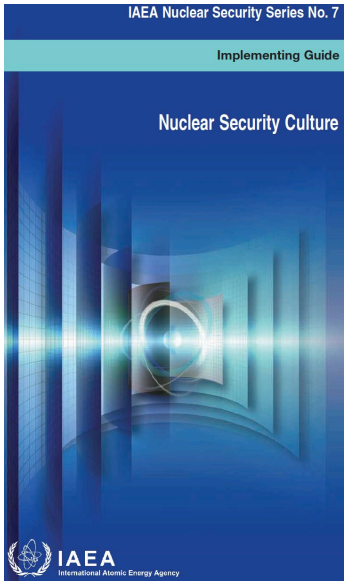


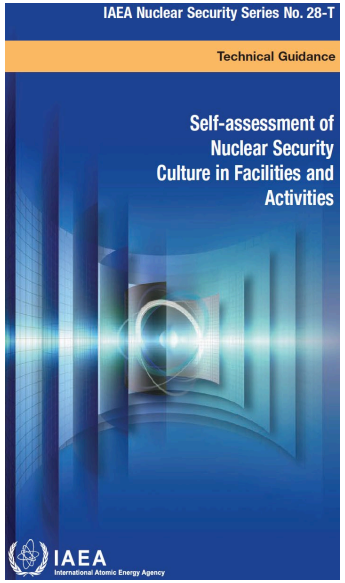
IAEA Foundations

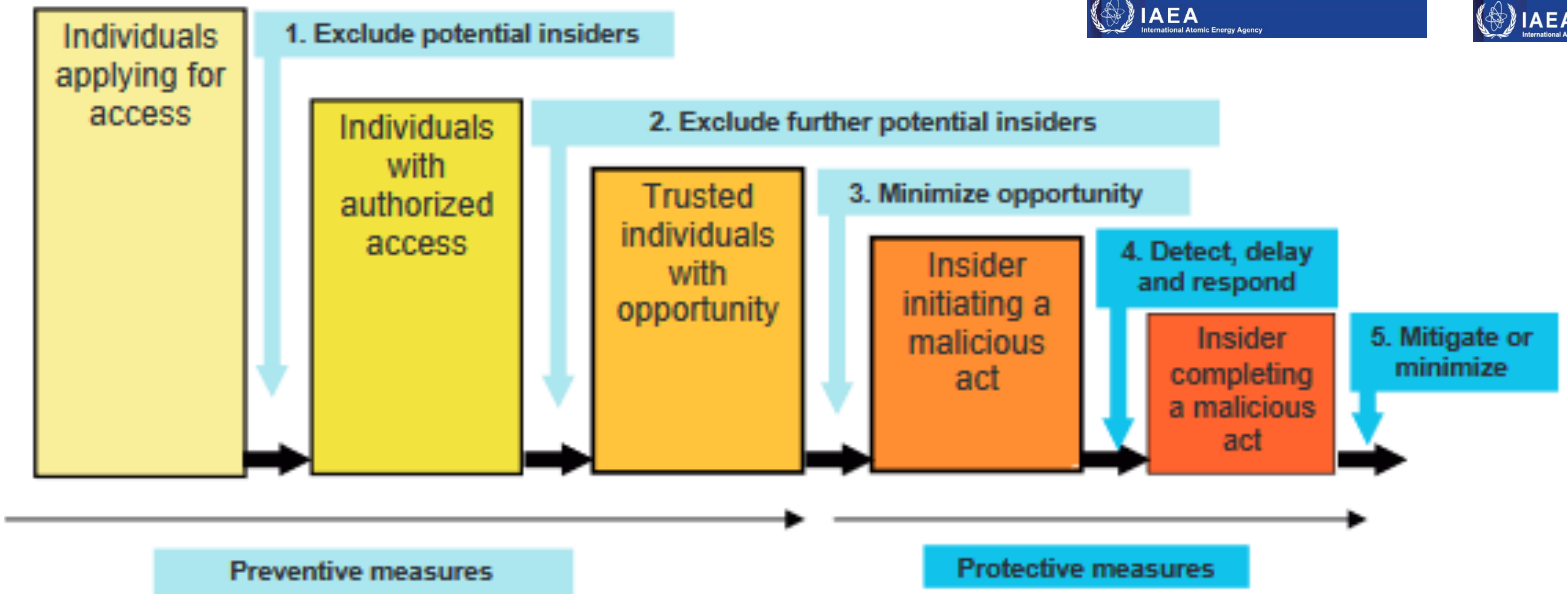
People & Culture

Personnel

Culture







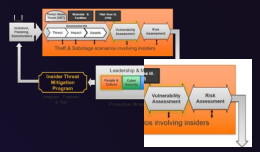
A lot of tools to help with assessments have been developed:

- Physical Systems Tools:
  - Force on Force Tools
  - Path analysis tools (single path, multi path)
  - Scenario analysis tools
  - Simulation tools
  - Visualization tools
  - Teaching/awareness tools
  - Table top exercises
- Cyber Systems Tools:
  - Path analysis tools for cyber
  - (and all the other tools used for physical)
  - Traps
- Data Analysis tools
- Forensic tools

List of Tools Available for INS Insider Toolbox

Tool	Category	Owner
ASSESS (Analytic System and Software for Evaluating Safeguards and Security)	Vulnerability Assessment/path analysis	LLNL
AVERT	path analysis and simulation tool	ARES Corp.
CDC –CHEM Prototype VAM	Vulnerability Assessment	U.S. DoJ
BattleBoard	Table Top exercise	ORNL
EASI/EPIT:	Single path analysis	
DBT (Design Basis Threat)	Threat Assessment	IAEA
Discrete Event Simulation Software	Discrete event simulation/Process simulations	Commercial -Many
FMEA (Failure Mode Effects Analysis)	Failure mode effects analysis methodology	Many
IPAD (Integrated platform for the analysis and design)	Simulation & path analysis	R&D
ITAT	Vulnerability/Path Awareness Table top exercise	Y-12
ITVA - Tanager:	Insider Threat Vulnerability Assessment	Tanager Inc.
NUSAM (Nuclear Security Assessment Methodology)	Security Assessment methodology	IAEA
RAM-tool	Risk assessment Tool/methodology	SNL
Decision Tree Maker/Creator Tools	Knowledge capture methods/tools	Commercial and freeware
ProEv	Path analysis (multipath)	Czech Republic
Process/Procedures Matrix	Procedure Assessment	SNL
QSAR: (quantitative security risk assessment)	Assessment methodology	R&D
SAPE	Vulnerability assessment & sensitivity analysis	R&D / Korea
SAVI (Systematic Analysis of Vulnerability to Intrusion)	Path analysis (multipath)	SNL
SCRIBE	Vulnerability/Path Visualization/Awareness	
Vanguard/SIMAJIN/PACRAT	Human out of the loop simulation	RhinoCorp.
SNL TTX	Vulnerability/Path Awareness Table top exercise (a method, not a tool)	SNL
STAGE: Scenario Toolkit Generation Environment)	Simulation-scenario analysis-security evaluation	Presagia (Canada)
VEGA, VEGA-2	Both a multi-path analysis and simulation tool)	Eleron/Rosatom
VISA & MP VISA	Path analysis tool (VISA-1 path; MP VISA-multipath), security effectiveness analysis tool	
VISA-2	Vulnerable path analysis; developed for NRC	NRC

INS Tool Box Needs: Vulnerability Analysis Tools



- Tools designed for insider threats, capabilities, goals
- Tools designed for MULTIPLE insiders
- Tools for better insider/outsider collusion
- Tools that go beyond pass/fail:
  - margin to failure
  - defense in depth—tools that allow for analysis with critical security element bypassed by insider
- Tools to better capture & use brainstorming of what an insider could do
- Tools to better capture uncertainty

- Methods for testing, evaluating, comparing, validating different assessments & assessment tools.

Summary

Building INS Toolbox for ITMP

- Top-level/Broad resources:

Plethora of well-developed available tools, frameworks, roadmaps, guides, best practices, standards for addressing insider threats (but not specific to nuclear.)

- Develop a ITMP process for international engagement
    1. Education: Insider awareness education – the threat is real!
    2. Initiation: help establish leadership, management, roles/responsibilities
    3. Implementation: workshops on specific components, tools, resources
    4. Evaluation: threat/vulnerability/asset/risk assessments tools & aids
    5. Improvement: Engagement on improving tools, incorporating lessons learned
- Harmonize tools for the toolbox with INS, WINS, IAEA, International standards **&** information security/cyber security insider threat standards.
- Optimize tools for INS engagement in each country