INSIDER THREAT MITIGATION

AN INTERNATIONAL SYMPOSIUM

Brussels 2019

CO-HOSTED BY

NNSA
National Nuclear Security Administration

FANC
federal agency for nuclear control

INSIDER THREAT MITIGATION

Table of Contents

> ***"The insider threat is real, and pervasive. This threat cannot and will not go unaddressed."***
>
> Pieter De Crem, Belgian Minister for Security and Home Affairs

INTRODUCTION

The United States Department of Energy and the Belgian Federal Agency for Nuclear Control, in cooperation with the International Atomic Energy Agency (IAEA), convened the inaugural International Symposium on Insider Threat Mitigation in Brussels, Belgium during 12-14 March 2019. The purpose of the symposium was to support the 2016 Joint Statement on Mitigating Insider Threats (INFCIRC/908) and develop and foster an integrated insider threat mitigation strategy for the nuclear security domain.

In 2016, recognizing the international community's need to address the insider threat, the United States sponsored IAEA Information Circular 908 (INFCIRC/908) – Joint Statement on Mitigating Insider Threats, which now has 29 countries and INTERPOL as signatories. This joint statement seeks to "build awareness of and acknowledgement that the insider threat is credible and that they pose a serious threat to the security of nuclear and other radioactive materials." The International Symposium on Insider Threat Mitigation creates a forum for discussion and action on this important topic within the international community.

OBJECTIVES

Insiders pose a significant threat to nuclear/radiological security, as they generally possess access rights which, together with their authority and knowledge, grant them far greater opportunity than outsiders to bypass dedicated nuclear and radiological security elements.

Through the lens of nuclear security, the symposium provided a forum to:

1) Raise awareness of the insider threat to nuclear and radiological facilities, and nuclear and other radioactive materials while in use, in storage, or during transportation
2) Exchange information on best practices and lessons learned when developing and implementing insider threat mitigation programs at the national and facility levels
3) Foster a common understanding that key elements of effective insider threat mitigation are similar for both nuclear and radiological facilities, recognizing that the implementation of respective practical measures may be different
4) Promote implementation of insider threat mitigation measures
5) Showcase commitments made per INFCIRC/908 and encourage future endorsements of INFCIRC 908

KEY THEMES

> *"Radicalization is unhappiness hijacked by ideology"*
>
> Paul Van Tigchelt, Keynote Speaker

Motivation and Intent

In this roundtable, panelists identified who and what are insider threats and what motivates this behavior.

Insider threats do not discriminate, they can be found in all industries and around the globe. Personal and organizational motivations for insiders vary and can include greed or financial desperation, family or workplace stress, disgruntlement, and job insecurity. Coupled with psychological or behavioral issues, when triggered, these insider characteristics can be expressed in the workplace as acts of theft, sabotage, espionage, or violence. Severely distressed and vulnerable individuals are at high risk for coercion or even radicalization. Warning signs, such as changes in behavior or outbursts at work must be addressed.

Key takeaway: Anyone has the potential to become an insider threat. Effective insider threat mitigation measures and organizational interventions must be robust; they include increased awareness and training, support and resources for at-risk employees, the use of risk management tools, and behavioral models to quickly identify and address aberrant behavior.

"It takes a network to defeat a network"

Paul Van Tigchelt, Keynote Speaker

Strategies and Challenges

Regulator, operator, and industry offered their insight and perspectives on insider threat mitigation tools, processes, and challenges they have encountered at nuclear and radiological facilities around the world. Presentations included numerous case studies and lessons learned. The speakers had a broad experience base, which ranged from starting the implementation of an insider threat mitigation program to maintaining an established, robust system.

From the U.S. viewpoint, the Nuclear Regulatory Commission provided a historical overview of its program and the struggles it faced during the legislation and codification stages, which are usually required to take place publicly. Meanwhile, industry described its commitment to global security culture, which requires strong physical security elements, personal attitudes, security hygiene and procedures, and end of life management.

The Belgian regulator and operator conducted a joint presentation to describe an insider incident at a domestic reactor, which caused significant property damage. The need for an insider threat program was recognized. However, the incident has increased awareness and vigilance. Also, the number of measures implemented by the ITM program greatly increased and expanded to not only nuclear sensitive areas.

The Finnish described trustworthiness mechanisms, such as security clearances and vetting, which are available through various government security services. These devices are integral for creating a comprehensive mitigation program.

Indonesia has reacted to its IAEA IPPAS missions at its research reactors by fostering a nuclear security culture, strengthened by procedures such as self-assessments and supported by interagency cooperation.

Cross-Industry Comparative Analysis

In this panel discussion, representatives from law enforcement, the chemical industry, diamond market, biological research laboratory and the oil and gas sector discussed insider threat mitigation measures and challenges.

Every industry has materials, data or information, which if lost, stolen, or damaged, could result in serious consequences. While the specific consequences may vary (e.g., environmental damage, loss of profit), the likelihood of a successful insider event is viewed as relatively low. Trusted insiders with the appropriate motivation have the potential to infiltrate an organization. There are currently no standardized personnel vetting programs to identify insiders before hire, monitor them during employment, or after they have left an employer. Additionally, some industries lack clear, authoritative, legislative frameworks to prosecute insiders or share the names of blacklisted persons. Maintaining a healthy security culture with rules and procedures is critical. In addition, developing good business practices such as removing access to physical spaces and computing resources immediately after a person leaves the organization can limit a disgruntled employee's ability to do harm.

Key takeaway: Insider threat mitigation measures used by different industries are target agnostic. Additional opportunities for multidisciplinary perspectives to share good practices and insider threat mitigation strategies are warranted and encouraged.

International Engagements

In addition to the United States' sponsoring INFCIRC/908 and Belgium's co-hosting the symposium, others in the international community have promoted the importance of insider threat mitigation, namely by subscribing to the Joint Statement or agreeing to hold events on the topic. The purpose of this session was to offer partners the opportunity to inform an international audience of resources available outside of the symposium's cohosts.

While Argentina has not yet become an INFCIRC/908 subscriber, the country collaborated with U.S. DOE's Office of International Nuclear Security (INS) to conduct a Latin America regional insider threat mitigation training. Meanwhile, the IAEA has launched a number of insider threat mitigation efforts, such as the coordinated research project on Preventive and Protective Measures Against Insider threat at Nuclear Facilities and also a series of international trainings, including the Advanced Practitioner-Level Training Course at Sandia National Laboratories in July. Morocco's National Center for Nuclear Energy, Sciences, and Techniques is collaborating with INS to hold in Rabat during June an Africa regional insider threat workshop. The Japan Atomic Energy Agency's Integrated Support Center for Nuclear Nonproliferation and Nuclear Security provides a variety of related trainings year-round to Asian countries. The United States and Belgium continue to encourage their international colleagues to consider either attending one of these events or even hosting one.

Over-the-Horizon: Future Considerations for Insider Threat Mitigation

In this panel discussion, emerging insider threats and mitigation strategies for those threats were discussed.

The online cyber-landscape is evolving at a phenomenal pace. New platforms for online communications such as mesh networks, peer-to-peer software, and the dark web enhance anonymity and privacy. At the same time, these technologies make it easier for insiders to be recruited or coerced by external parties. Providing employees with access to only the information needed to perform their jobs is critical. Monitoring employee user activity and maintaining awareness of external resources being accessed through firewalls facilitates the creation of baselines. The baseline is a unique fingerprint of web-activities which can be used to block unsecure or illegitimate processes, watch and wait, or facilitate rapid response to a potential data exfiltration. Training staff on how and why to protect data, rules for safe and legitimate computer access at work, and how to identify online spoofs and phishing campaigns are critical.

Insider threat mitigation programs will not all look the same due to differences in industry, culture, privacy laws, past security issues, and computing resources. While tragic events often drive organizational change, the more proactive we are about identifying where the next threat will come from, the better we will be able to respond.

> *INFCIRC/908 subscriber leadership and commitments are commendable, and other countries are encouraged to consider endorsing this very important Joint Statement.*
>
> Art Atkins, Facilitator, INFCIRC/908 Panel

INFCIRC 908: A Global Tool to Advance Insider Threat Mitigation

In 2016 on behalf of the governments of 26 countries and INTERPOL, the United States issued a Joint Statement, "Mitigating Insider Threats," as IAEA Information Circular 908 (INFCIRC/908). INFCIRC/908 records the intent of subscribing governments to establish and implement national-level measures to mitigate insider threats. It also documents their commitment to supporting the IAEA in developing and implementing an Advanced, Practitioner-level Insider Threat Mitigation training course, and their dedication to undertake measures that counter insider risks, using a risk-informed and graded approach. The symposium showcased the commitments by subscriber countries as set forth in INFCIRC/908, as well as those in the process of subscribing.

Since 2016, many commitments have been made to advance insider threat mitigation for nuclear security. The commitments include convening regional workshops for operators, law enforcement, regulators and others; launching relevant training programs; implementing recent regulatory guidance which require vetting and reliability programs; and establishing an insider threat mitigation program within a national legal framework. Challenges to meeting the commitments are manageable and may take some time to be resolved. Key challenges include: bringing together stakeholders to engage on insider threat mitigation; implementing an human reliability program which is relevant to the nuclear community; improving nuclear security culture, integrating database management; and strengthening coordination across all national stakeholders.

INFCIRC/908 is a global tool to advance insider threat mitigation. Promoting INFCIRC/908 at the regional level was viewed as practical measure because regional workshops have been effective in showing "we are not alone" in addressing this issue and sharing good practices with countries that have similar culture and language is invaluable. Meeting the commitments of INFCIRC 908 advances the capabilities and parity of the international insider threat community, provide credibility on insider threat mitigation when engaging with other subscribing countries, and may also serve as a security deterrent.

Subscriber leadership and commitments are commendable, and other countries are encouraged to consider endorsing this very important Joint Statement.

> ***"….We are acutely aware of the consequences…There is no room to be complacent. Simply put, we must stay ahead of the threat."***
>
> Lisa E. Gordon-Hagerty, Under Secretary for Nuclear Security and National Nuclear Security Administration Administrator, United States Department of Energy

FOCUS AREAS FOR THE FUTURE

National Policy and Regulatory Frameworks

This session was designed to engage participants in the discussion of the role government agencies have in mitigating insider threats at nuclear and radiological facilities, and how to address insider threats within a national regulatory framework.

During this breakout session, participants were divided into groups of 4 to 5 people and asked to discuss and out-brief one of eight topics listed below:

1. What are the regulatory requirements to mitigate insider threats in your country, and are international guidance documents taken into account?
2. How is communication organized between all involved State stakeholders and operators?
3. What is the role of the Design Basis Threat (DBT) in insider threat mitigation?
4. Who is responsible to coordinate actions when first signs of an insider are detected/reported?
5. Does vetting for trustworthiness need to be taken into account in a regulatory framework and how?

6. What are the challenges in creating a national policy to implement an insider threat mitigation program?
7. Which stakeholders are involved in an insider threat program (incident, vetting, etc.)?
8. Who is best positioned to make decisions on how to handle a possible insider – operator or state level, and why?

This session allowed individuals from different countries to discuss if and how insider threat programs are addressed within the national regulatory framework, what challenges there are to coordinating government agencies to respond to insider threats, and what might be done to overcome these challenges.

Some areas for further exploration that came out of this session include:

- The need to have a design basis threat for insider threats;
- The challenge of consensus and approvals for a national insider threat mitigation policy; defining how to identify and respond to concerning behaviors;
- Overcoming cultural challenges;
- Defining the intersection between safety and security cultures;
- The challenge of developing a regulatory framework that allows for a graded approach and gives operators some decision-making ability in implementing insider threat measures.

Nuclear Security Culture

The nuclear security culture interactive session was designed to explore why security culture weaknesses can manifest and how to identify strategies for enhancement.

Using the IAEA nuclear security culture framework outlined in the IAEA Nuclear Security Series No. 7 (NSS-7), "Nuclear Security Culture," this interactive session engaged participants in simple scenario analysis through structured brainstorming. Audience members were divided into small groups of 4-6 persons.

A short vignette about a fictional company, its personnel, management practices, and security posture was presented. Each team was asked to conduct a security culture assessment, identify specific weaknesses within the company, and recommend improvements required to enhance the security culture and mitigate insider threats.

The teams were each provided with a game board and deck of cards. The game board utilized the iceberg concept to highlight the tangible, or visible characteristics (e.g., tools, policies, and technical measures) and the intangible, or invisible (i.e., beliefs, attitudes) characteristics of nuclear security culture. Cards, with visual representations of these characteristics, were selected by team members and placed on the board to illustrate the current-state and the desired future-state of the organization.

The goals of the session were two-fold: encourage healthy dialog and debate on the topic of insider threat, and raise awareness of how generational, cultural, and professional differences impact an organization's security culture. Participants reflected that management buy-in is key to enacting culture change. Regular and consistent security training needs to be developed and implemented with tailored training for those in critical roles. Security and non-security personnel must maintain close and ongoing interaction and shared design of security protocols to avoid organizational conflicts. Finally, security culture must evolve with the organization to address the use of new technology, generational norms and expectations, and the impact personal attitudes and beliefs have on individuals, groups, and the entire workforce.

Next steps:

- Provide training and assistance on how to improve communications between security and non-security personnel on the insider threat topic.
- Identify critical and/or sensitive worker roles germane to multiple industries and develop specialized insider threat training.
- Help organizations develop skills to communicate the importance of a strong security culture to upper management and how to convey the positive contributions it will make to insider threat mitigation.

> *"Disgruntlement matters and simple steps can make a difference."*
>
> Matt Bunn, Keynote Speaker

Cybersecurity

An interactive parallel session on cybersecurity and the insider threat employed a real-life case study. The takeaways from the session were to make the participants more aware of what constitutes a cyber insider, how an insider can exploit information security, and measures that can be put in place to mitigate the cyber insider threat. The goal of the session was for the participants to provide examples of how a cyber insider threat vulnerability can be mitigated.

The session used a case study on a cyber incident at the Davis-Besse Nuclear Power Plant (NPP) taken from a magazine article written by Kevin Poulsen, SecurityFocus, "Slammer worm crashed Ohio nuke plant network" published in August 2003.

The participants were asked to answer the following questions for the case study scenario.

- Is there a "cyber insider" at work in this incident? If so, who?
- Was the insider "Witting" or "Unwitting"?
- What mitigation steps might be utilized to protect from this in the future?
- What additional cybersecurity policies, procedures, or controls does your facility have in place that would have prevented this situation from occurring or would have detected this network configuration in a timely manner?

The Davis-Besse NPP case study involved an intrusion through multiple IT systems of a malware threat that compromised the plant's Safety Parameter Display System. The worm was introduced onto the site by a subcontractor that established a network connection of which the plant IT staff was unaware.

The groups were split on whether there was an insider and if the insider was unwitting or not. The group discussed tools to address vulnerabilities and mitigation steps, these included training/culture, procedures, and network isolation. In addressing the groups' current systems/networks, it was noted that in

2002 the focus was on networking as much as possible, and in today's world, we focus on enterprise management, content monitoring, and the need for layered approach to cybersecurity controls.

The session also had discussions on what an insider is and who was involved in creating the vulnerability at the Davis-Besse NPP. A key finding of the session was the need to include cybersecurity policies and requirements in subcontracts to help ensure vendors do not introduce cyber vulnerabilities.

Next Steps

The participants discussed how they could apply the knowledge and awareness of cybersecurity from the session into their own facility operations. The exploitation of cybersecurity with insider threats was also recognized to blur the conventional distinction between insider and outside threats to a facility. For example, coupling cybersecurity elements with an insider threat potentially broadens the community of malicious actors, because not all malicious actors need be physically located on the affected site. A malicious actor with insider information, but located on the outside of a facility, could wreak havoc on internal systems and protocols from a remote location. As such, this notion of how insiders exploiting cybersecurity elements could impact current mitigation paradigms and norms warrants further exploration.

"The definition of insider threat is comparable across all sectors."

ir. Yvan De Mesmaeker, Facilitator, Cross-Industry Comparative Analysis

Trustworthiness and Aftercare

This interactive session included subject matter experts and an actor, depicting specific behaviors which may indicate potential disgruntlement, or even radicalization, in an employee. Using a specific scenario, the participants, divided into smaller groups, received a specific role and a different 'sign of change in behavior'. Based on this information they discussed if the person could pose an concrete insider threat and if they needed to take action in this situation.

In general, one 'sign of changing behavior' did not trigger any action, nevertheless when all signs were taken together, the participants decided to confront the person about the gathered information. This confrontation was played out by one of the participants and the actor.

The use of an actor allowed for the quick inclusion of many examples of behavioral change, taking account cultural influences and organizational policies and regulations. The subject matter experts facilitated the discussion, highlighting the importance for management to observe and report, not to diagnose.

The discussions during these sessions indicated why a general approach on this topic is very difficult, and more specifically:

- Cultural challenges due to organization, local laws, policies and regulations.
- Difficult balance between trust and reporting
- Roles and relationships determine how you address the situation

Next Steps:

- Guidance in how to follow up and address changes in behavior that can be adapted to specific countries.
- Structured list on behaviors of concern for screening and for continuous monitoring.

Technical Measures to Mitigate Insider Threats

In this session, two scenarios were presented, one included an event at a research reactor and the other at a medical facility utilizing irradiated blood which required radioactive sources. The facilitators described the scenario and each group was tasked with enhancing the technical measures to better secure the facility and mitigate the threats posed by the disgruntled insider. The scenarios came to life with a two-dimensional facility lay-out with physical security tools available for "purchase" with fictitious funding, mirroring the types of decisions companies or facilities may be facing. The groups identified innovated and creative approaches to mitigating potential threats by leveraging technology, either as a deterrent or as delay mechanism.

Next Steps: This approach could be easily replicated and, based on the interactions of the participants, it seemed to resonate very well in a workshop setting. Tailoring the scenarios and facilities will be important and will certainly inspire creative approaches with technology to mitigate potential insider threats.

> *"Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning"*
>
> Winston Churchill

CONCLUSION AND NEXT STEPS

The symposium participants concurred that two efforts should move forward to help advance and promote our international community on insider threat mitigation for nuclear security:

1. Stand up an "Advancing Insider Threat Mitigation (INFCIRC 908) Working Group"
2. Conduct a Side Event on the 2019 Insider Threat Mitigation Symposium at the IAEA International Nuclear Security Conference in February 2020

Advancing Insider Threat Mitigation (INFCIRC 908) Working Group

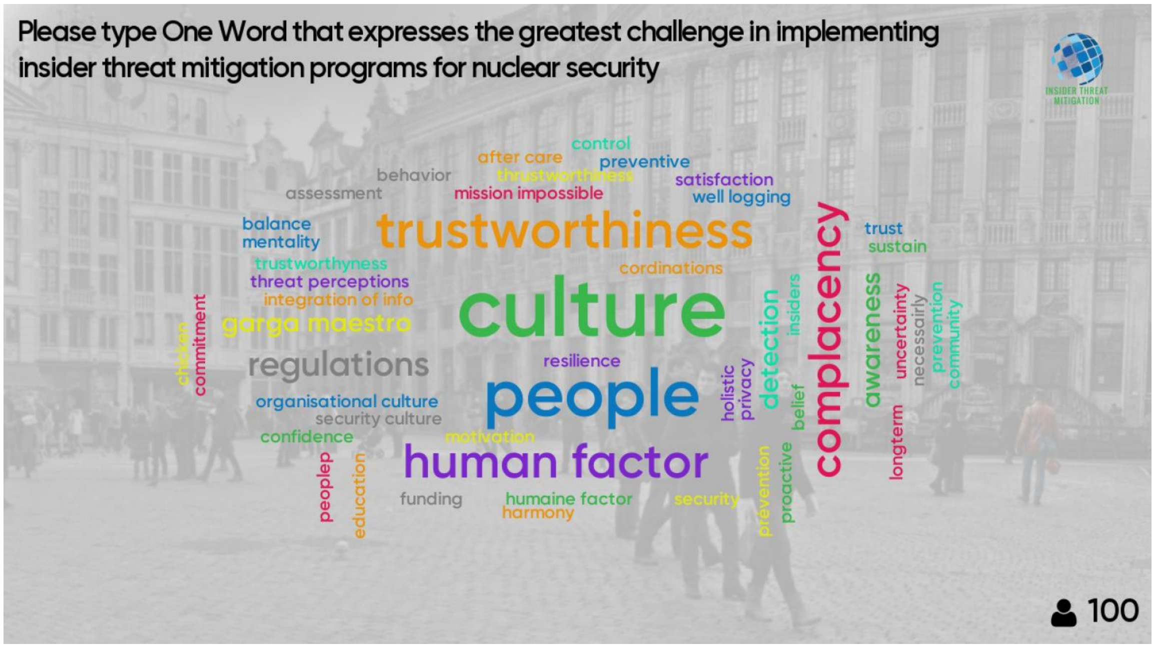
A Terms of Reference for this working group will be drafted by late 2019. It is anticipated that areas for the working group would include (but not limited to): Establish Focus Groups to explore key themes and issues from the Symposium, Promote an outreach strategy to showcase INFCIRC 908 commitments; Develop opportunities to share experiences and best practices on implementing insider threat mitigation programs; and Create a calendar of insider threat mitigation events and activities for the international community. The Terms of Reference will also address working group objectives, tasks, membership, and governance.

Side Event at 2020 IAEA Nuclear Security Conference

The next IAEA International Nuclear Security Conference will be held 10-14 February 2020 in Vienna, Austria, which is convened approximately every three years. A Side Event was proposed and discussed as an effective way to showcase the key themes and outcomes of this symposium. The Side Event would also highlight and recognize the INFCIRC 908 commitments being made by Member States as well as notable achievements by the insider threat mitigation international community.

Details about a proposed Side Event on the International Symposium on Insider Threat Mitigation will be forthcoming.

The participants also provided one word that expressed their thoughts on the greatest challenge in implementing insider threat mitigation programs for nuclear security. The resulting word cloud is shown in Figure 1.



Please type One Word that expresses the greatest challenge in implementing insider threat mitigation programs for nuclear security

Figure 1: Anonymous polling question posed to the participants at the Insider Threat Mitigation Symposium, Brussels, Belgium, 12-14 March 2019

APPENDIX I: LIST OF PARTICIPATING COUNTRIES

1. Albania
2. Angola
3. Argentina
4. Austria
5. Bangladesh
6. Belarus
7. Belgium
8. Burkina Faso
9. Cameroon
10. Canada
11. Chile
12. China
13. Czech Republic
14. Democratic Republic of Congo
15. Egypt
16. Finland
17. France
18. Germany
19. Ghana
20. Indonesia
21. Iraq
22. Israel
23. Italy
24. Japan
25. Jordan
26. Republic of Korea
27. Lebanon
28. Libya
29. Malaysia
30. Mauritania
31. Morocco
32. The Netherlands
33. Nigeria
34. Peru
35. Philippines
36. Poland
37. Republic of Moldova
38. Singapore
39. Slovak Republic
40. Slovenia
41. South Africa
42. Spain
43. Sweden
44. Switzerland
45. Thailand
46. Tunisia
47. United Kingdom
48. Ukraine
49. United Arab Emirates
50. United States of America
51. Vietnam
52. Zambia

APPENDIX II: IAEA INFORMATION CIRCULAR 908 (INFCIRC 908)

22 December 2016

This joint statement records the intent of Armenia, Australia, Belgium, Canada, Chile, Czech Republic, Finland, Georgia, Germany, Hungary, Israel, Italy, Japan, Jordan, Kazakhstan, Mexico, Morocco, the Netherlands, Nigeria, Norway, Republic of Korea, Romania, Spain, Sweden, Thailand, United Kingdom, United States and INTERPOL to establish and implement national-level measures to mitigate the insider threat.

Insiders generally possess access rights which, together with their authority and knowledge, grant them far greater opportunity than outsiders to bypass dedicated nuclear and radiological security elements or other provisions such as safety systems and operating procedures. Insiders, as trusted personnel, are capable of methods of defeat that may not be available to outsiders. As such, insiders—acting alone or in concert with outsiders—pose an elevated threat to nuclear security.

To establish an integrated, graded approach to mitigating insider threats, nuclear and radiological security programs should include national-level and agency- or facility-specific Insider Threat Mitigation policies and programs, training and awareness activities, and collaboration between facility-level organizations. The Insider Threat Mitigation Program should include strong control and accountability measures for special nuclear material that rigorously assess and continually monitor insider human reliability, deter insiders from theft/diversion, limit their access, and provide prompt detection of theft/diversion.

1. **States commit to supporting the International Atomic Energy Agency (IAEA) to develop and implement an advanced, practitioner-level training course on preventive and protective measures against insider threats.**

The IAEA, with the assistance of Member States, has developed and implemented a basic training course to help mitigate insider threats. With support from partner Member States, and in response to IAEA basic insider threat mitigation course participant survey responses, States will support the IAEA with the development of an advanced, practitioner-level training course on preventive and protective measures against insider threats. This more advanced course will provide member states with hands-on training, guidance documents and related self-assessment and training materials. Similar in format to the IAEA's International Training Course on Physical Protection, the course could be piloted in Member States with appropriate facilities, and then transitioned to Nuclear Security Support Centers and Centers of Excellence (NSSC/COEs) in partner States. The training course will focus on physical protection of materials, facilities, and sensitive information from insider threats, as well as Nuclear Material Accounting and Control (NMAC), trustworthiness program, nuclear security culture, and other methodologies to protect against theft of nuclear materials and sabotage of facilities. Future instructors from NSSC/COEs would receive special preparatory training, and then help teach the pilot course and both regional and national NSSC/COEs may adapt the courses as appropriate to meet the threat-based needs of the Member States.

2. States will implement measures to mitigate insider risks using a risk-informed graded approach by taking actions that may include one or more of the following:

- Developing and implementing a national-level policy on insider threat mitigation, identifying all relevant stakeholders and information sources, and implementing agency-specific training and education.

- Developing or maintaining an outcome focused regulatory approach that will assist those responsible to think more holistically about security risks and mitigations.

- Taking specific steps to facilitate collaboration and information sharing among relevant national organizations (e.g., facility security, human resources, personnel security, national security, counter-intelligence and law enforcement).

- Establishing or strengthening NMAC programs for nuclear security purposes, and regulations for implementation, including, for example,
    - Systems to identify nuclear material status, movement, and changes. These may include appropriate NMAC software, secure electronic data transfer between facilities and to the national or regional level, and established national- or regional-level plans to respond to suspected theft/diversion;
    - Facility-level Material Control & Accountability (MC&A) programs to detect theft/diversion through modern nuclear material accounting system software, including peer review of software;
    - Regional-, National-, and facility-level programs to conduct performance tests, self-assessments and peer reviews to assess and enhance effectiveness of insider threat mitigation programs to include NMAC systems.

- Establishing a nuclear security regime for protection of materials and facilities from insider activities, including, for example:
    - Development and implementation of a training program to mitigate insider risk to include topics such as the importance of the individual in recognizing and preventing insider threats; physical protection systems used to secure materials at facilities and in transit; insider analysis, prevention, and mitigation; and how to develop trustworthiness programs;
    - Physical protection systems used in protection of materials and facilities;
    - Nuclear security culture;
    - Methodologies to protect against protracted and abrupt theft of nuclear materials;
    - Procedures for materials transfer;
    - Protection of materials at the target;
    - Access (e.g. two-person) rules and other administrative and technical measures against insider threats;
    - Defined physical protection design objectives and/or measures as they relate to sabotage and the potential insider threat; and
    - Maintaining good cyber hygiene procedures such as protective monitoring on cyber estate and ensuring user privileges are relevant and appropriate to their current role.

- Establishing insider trustworthiness programs that can include:
    - Defining eligibility requirements;
    - Clearly identifying and documenting roles and responsibilities;
    - Conducing background checks;
    - Initial and ongoing:
        - Vetting of personnel by law enforcement agencies;
        - Medical and psychological testing;
        - Drug and alcohol testing;
    - Detecting and reporting aberrant behavior;
    - Process for no-fault self-reporting any condition that may affect an individual’s ability to conduct security responsibilities and for reporting any other security concerns;
    - Providing personnel assistance programs to help mitigate life stressors that can impair ability to conduct security duties; and,
    - Regular security awareness training, including cyber security.