World Institute for Nuclear Security

Workshop on Understanding and Mitigating the Insider Threat

Abu Dhabi, UAE. 16 – 18 December 2018.

Report

BACKGROUND

Nuclear operators seek to employ personnel who can be trusted with sensitive information, critical technology, and hazardous nuclear and radioactive materials. This requires employees who are honest, dependable and mentally and physically stable. Social backgrounds and external influences, as well as a host of other influential factors, can create undue levels of vulnerability, altering a person's dependability, moral character, motivations and allegiances. History has repeatedly shown how such changes have catalysed insider threats and weaknesses in nuclear safety and security, sometimes leading to serious consequences.

Past incidents have clearly demonstrated that insiders can take advantage of their access rights and knowledge of a certain facility, as well as their authority over staff, to bypass dedicated security measures. They can also threaten cybersecurity, safety measures, and material control and accountancy (MC&A). Insiders are likely to have the time to plan their actions; in addition, they may work with others who share their objectives. Employees may sometimes also cause harm unintentionally, particularly in the cyber realm. Finally, no matter how serious the threat from outsiders may be, it can be leveraged or multiplied through the help of one or more insiders.

In order to further explore the topic and contribute to the collective efforts aiming at mitigating the insider threat, the World Institute for Nuclear Security (WINS) and the Federal Authority for Nuclear Regulation (FANR) decided to partner and organise a joint workshop from the 16th to the 18th of December 2018 in Abu Dhabi, UAE. This international event focused on the measures to prevent, detect and respond to insider actions. It was attended by 54 delegates from 15 countries and 2 international organisations who represented key nuclear security stakeholders, in particular regulatory agencies and nuclear operators.

OVERVIEW OF THE EVENT

This interactive, professionally facilitated event was built around a number of presentations from invited Emiratis and international expert speakers. It included a tabletop exercise (TTX) and breakout sessions that enabled participants to further explore certain topics and listen to each others' experiences. In addition, an instant electronic voting system was used to allow participants to anonymously share their views on selected questions related to insider mitigation matters.

A primary objective of the event was to examine the latest and most effective methods to assess and manage insider threats. Consequently, the workshop agenda covered programmes and tools developed to ensure the reliability of personnel accessing critical areas or information and explored the role and contribution of different stakeholders involved in the identification and mitigation of internal threats. Examples of specific topics addressed during the workshop include:

- How the insider threat landscape has evolved in the last few years.
- The process for identifying the motivation, intention and capabilities of insiders.
- Real-life examples and applicable case studies.
- The key components of insider mitigation programmes, with a focus on human reliability and employee satisfaction programmes.
- Methodologies and metrics for measuring the performance of the insider mitigation programme and for sharing best practices for reporting it to senior management.
- The importance that individuals throughout the organisation participate in identifying and responding to credible threats.

WORKSHOP PROGRAMME

SUNDAY 16 DECEMBER 2018

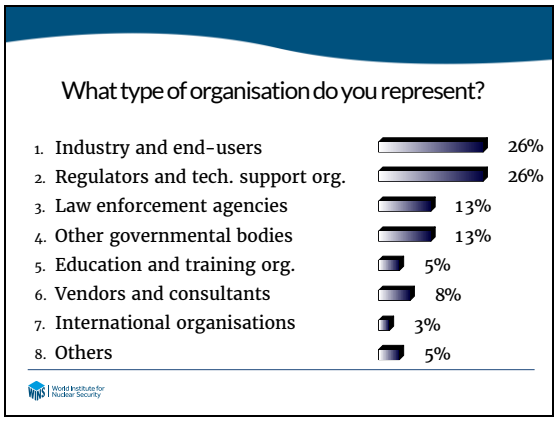
OPENING SESSION

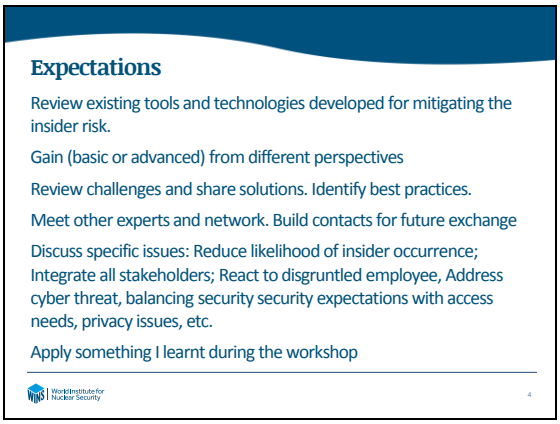
Mr Raoul Awad, Deputy Director General for Operations, FANR (UAE) opened the workshop by reminding the group of the long-lasting collaboration between WINS and his organisation and by highlighting the credibility of the insider threat and the need for developing highly effective security arrangements. Placing this event into the UAE context, Mr Awad stressed the importance of bringing the different nuclear security stakeholders all together, ensuring their effective coordination and collaboration, and identifying and implementing improvements whenever needed or possible. He concluded his speech by wishing participants a fruitful workshop and encouraging them to share their practices, experiences and suggestions on mitigating the insider threat.

Mr Pierre Legoux, WINS Head of Programmes, then welcomed the participants on behalf of WINS, presented the objectives of the event, and provided a preliminary overview of the workshop agenda. Mr Legoux also displayed and commented on the most relevant results from the pre-workshop survey.

Participants' introduction and expectations

Participants were first asked to use the e-voting system to indicate which stakeholders they represent. Then they were asked to introduce themselves at their tables and discuss their expectations for the workshop.





SESSION 1 – UNDERSTANDING THE INSIDER THREAT

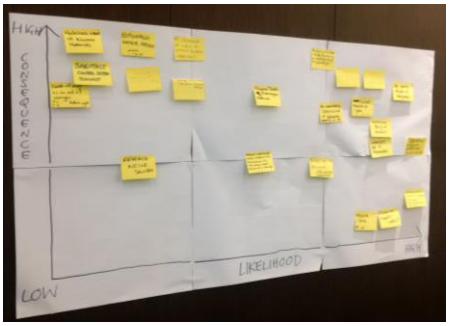
Session 1 gave the group an opportunity to discuss why the nuclear community is so concerned by the insider threat and how human attributes and characteristics impact security. It also included examples of actual insider cases in the nuclear industry and gave participants the opportunity to discuss which insider scenarios would be most likely to happen.

Mr Eric Lang from PERSEREC (USA) delivered a presentation on *Insider Threat: Social Science Insights and Applications.* Mr Lang began by reminding the group of PERSEREC's mission and research activities related to insider mitigation. He then reviewed usual motivation factors and provided examples of insider cases. Mr Lang stressed the importance for security professionals to understand human factors and to be aware that certain behaviours might be indicators of potential risks. He then provided some examples of good practices for mitigating the insider threat and walked the group through some barriers to effective implementation. Mr Lang concluded his presentation by providing some references for further reading.

During the follow-up discussions, Mr Lang discussed the role of technologies (important but not sufficient; predictive algorithms are still in the learning curve) and best practices for learning from past incidents. He also encouraged managers and staff to be proactive, not reactive to difficult personnel situations faced by their colleagues. Detection and incentive mechanisms exist, he said,

and should be used. People need to be aware of this and receive proper training on them. When an issue is identified, follow-up actions should be taken. Managers need to feel responsible, empowered to take actions and competent to take the best action. Since it is often a management issue, the HR Department should be deeply involved, if not leading the process.

Finally, at their tables, participants discussed what could be credible insider threat scenarios. They were encouraged to draft examples and place them on a consequence/likelihood scale. Suggested scenarios ranged from high likelihood/low consequences incidents, such as petty theft, to low likelihood/high consequences incidents, such as active shooter (revenge) or sabotage of IT&IC systems of a nuclear process.



SESSION 2 – ENGAGING ALL STAKEHOLDERS

Session 2 provided an overview of the objectives and content of an overall insider mitigation strategy and identified stakeholders involved in the mitigation process. It was also an opportunity to identify gaps and opportunities for optimising communication, coordination and cooperation amongst key stakeholders (e.g. the intelligence community, the regulator and the operator).

Mr Osama Alshehhi, FANR (UAE) opened the session by providing a regulatory perspective to insider mitigation. He defined what is meant by an insider and shared a few actual incidents to demonstrate. He then described the risk, as well as the role of regulatory agencies in mitigating it. In particular, he provided some details on relevant UAE regulations and described the overall protection strategy implemented in his country. Mr Alshehhi concluded his presentation by highlighting the importance of the regulatory oversight and inspection programme.

During the follow-up discussions, he mentioned some of the UAE's achievements, as well as some challenges that remain. Participants then participated in a discussion to identify other key external stakeholders with responsibilities for mitigating the insider threat and assessed their current contributions. They highlighted the fact that secrecy is still a barrier to effective communication, sharing of experience and—in some cases—transmission of important information among stakeholders. Some participants also challenged the effectiveness of mechanisms put in place to identify and share lessons learned from actual incidents. They said that in many cases proper follow-up actions are not taken. In addition, some participants mentioned how difficult it is to identify responsibilities in case of an insider action. (Is it a failure of the licensee? The vetting agency? Both?). Finally, participants agreed on the essential role that the regulatory agency plays in prescribing an operator's security performance objectives, conducting periodic inspections, and taking enforcement actions in cases of non-compliance.

In the last activity of the session, Mr Carl Reynolds, who facilitated the event, moderated a discussion with **Ms Assel Khamzayeva, IAEA Nuclear Security Division.** Ms Khamzayeva described the role that the IAEA plays, in particular her division, in insider mitigation and explained how participants could benefit from her participation in the event. Based on her experience, she offered feedback on strengths and weaknesses she has noticed amongst different countries and organisations with whom she has worked. She concluded by offering some advice to regulatory organisations and nuclear operators willing to enhance their contribution to insider mitigation.

During the follow-up discussions, participants highlighted cultural differences as a factor leading to strong variations among countries and organisations and the need for a clear legal framework for regulating trustworthiness checks and vetting activities. Participants also discussed additional topics, such as trust vs. verification, zero tolerance policies, and the difficulty of taking action on simple suspicions.

SESSION 3 – TABLETOP EXERCISE (TTX): SWEETBRIAR NUCLEAR POWER PLANT

To give participants an interactive starting point for workshop discussions and to review all areas to be addressed during the event, participants were asked to participate in a tabletop exercise simulating an insider scenario. They were asked to identify the actions a nuclear operator would likely take when responding to the incident and to mitigate possible consequences. The objectives of the TTX were structured around four phases:

- **Initial information** (stimulates thinking and the sharing of experiences and different perspective)
- **Incident response** (places insider mitigation measures into the workshop context)
- **An evolving situation** (highlights the importance of stakeholder engagement)
- **The recovery phase** (identifies strengths and weaknesses of measures put in place by participating organisations)

Carousel to review the TTX key findings and how they relate to the main sessions of Days 2 and 3.

To prepare for discussions covered in following sessions, participants were asked to split into six groups, each of which rotated through six working stations. The objective was to build on the key messages of the TTX and link their findings with the various sessions of the workshop. The topics addressed at the stations are summarised below. (Key findings of the carousel have been reflected in the various sections of the report addressing each topic.)

1. **Engaging and communicating with internal stakeholders**
   Who are the key internal stakeholders? What do they need to know? What information do they need to share? How satisfied are we with their involvement and contribution?
2. **Designing and implementing mitigation programmes**
   What are the essential elements of an insider mitigation programme? Which ones are in place and already effectively contributing to reducing the risk? Which ones are more challenging and need specific attention?
3. **Employee trustworthiness and reliability**
   What do we mean by trustworthiness and reliability? How is this achieved? What are we good at? What are the remaining challenges?
4. **Cyber insider threat**
   What are the specificities of the cyber insider threat? What are possible mitigation measures? What are we good at? What are the remaining challenges?
5. **Responding to an insider action**
   What needs to be in place to allow an effective response to an insider action? How can we practice response arrangements for insider actions? How often do we practice them? What are we good at? What are the remaining challenges?
6. **Measuring the effectiveness of insider mitigation programmes**
   What are the key indicators that would let us know that our insider mitigation programme is working? Which ones are easy to measure? Which ones are more challenging?

Mr Rony Dresselaers, FANC, Belgium concluded Session 3 and Day 1 with a presentation on *Dealing with Insider Threat in the Nuclear Industry*. Mr Dresselaers began by describing some usual insider profiles and a way to analyse the insider threat. He then provided more information on potential mitigation measures, including physical protection, trustworthiness verification and security culture. Mr Dresselaers concluded his presentation by highlighting some challenges that occur when designing insider mitigation programmes; he also mentioned several key success factors.

MONDAY 17 DECEMBER 2018

SESSION 4 – DESIGNING AND IMPLEMENTING MITIGATION PROGRAMMES AGAINST THE INSIDER THREAT

Session 4 identified and discussed the essential components of an insider mitigation programme. In particular, it provided the opportunity to further explore the role of a human reliability programme (HRP) and discuss practical and legal issues associated with implementing HRPs.

Mr Zaid Al Hebshi, ENEC (UAE) opened Session 4 with a presentation on the ENEC insider mitigation programme. After briefly introducing the audience to the vision and mission of his organisation, Mr Al Hebshi provided details on the elements of ENEC's security programme that help to mitigate insider risk. In particular, he described ENEC's overall physical protection approach and provided details on the procedures for authorising unescorted access, the fitness for duty programme, and cybersecurity arrangements.

Ms. Carol Higson, URENCO (UK) complemented Mr Al Hebshi's presentation by describing insider mitigation measures implemented by her organisation. After defining and explaining the role of personnel security, Ms Higson explained both overarching and specific objectives of Urenco UK's insider mitigation programme. She also provided some lessons learned from its implementation. Ms Higson concluded her presentation by encouraging participants to adopt a continuous improvement attitude and to pay more attention to the supply chain.

During the follow-up discussions, participants highlighted the importance of raising security awareness amongst all staff, in particular non-security professionals. It was stated that staff (colleagues) are often the first detection opportunity and should be educated to identify and report possible red flags. It was agreed that management was responsible for setting the rules and expectations for the insider mitigation programme and that staff should develop a sense of ownership and be a source of improvement should they identify gaps in the implemented arrangements.

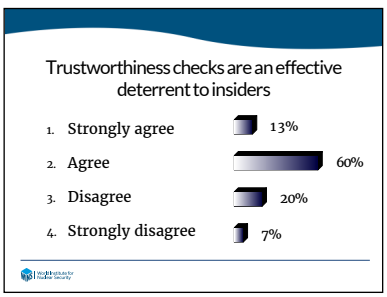
Participants agreed that the design and implementation of effective access control procedures is essential. Additional areas of agreement included that access control should follow a graded approach and comprise a mixture of procedural and technical measures. New technologies, such as biometrics and facial recognition, can bring significant improvement to access control procedures. It is important to record and analyse the access control data, in particular unauthorised access attempts. It is also important to know the false access acceptance rate. Access control authorisation should be linked to authorised working time. Emergency exit procedures need special attention. Tailgating should be prevented, and anti-pass-back should be implemented.

Participants also agreed that responding to an insider event is challenging, especially when the identity of the perpetrator has not yet been identified, and that any incident or significant dysfunction should be considered to be malicious until investigations have been conducted.

SESSION 5 – EMPLOYEE TRUSTWORTHINESS AND RELIABILITY

Building on the key findings of the previous discussions, Session 5 specifically explored the processes that should be implemented to ensure the trustworthiness of individuals with access to sensitive locations and information. In particular, the session enabled participants to share their vetting experiences and review and discuss factors that might influence the trustworthiness of individuals.

Session 5 opened with an E-voting question on the effectiveness of trustworthiness checks as a deterrent to insiders. The vast majority of participants agreed with the statement and indicated that although vetting is only one element of the insider mitigation programme, it is a necessary one. Participants clearly agreed that vetting is an effective tool for preventing individuals with known vulnerabilities or risks to be recruited or given access to sensitive areas and information. However, experience also shows that many incidents that have occurred at critical facilities have been conducted by vetted people.



Ms. Pinkie Rabali, Necsa (South Africa) shared her operational experience in her presentation titled *Vetting as a Primary Element Required in Ensuring Trustworthiness of Individuals Accessing a Nuclear Facility and Its Effectiveness*. Ms Rabali defined what vetting means, explained its purpose, and clarified what its expected outcomes are. She reminded the group of the importance and complexity of the legal framework applicable to vetting procedures and other screening activities. Ms Rabali concluded her presentation by offering some practical experiences in implementing vetting measures as part of a comprehensive insider mitigation programme.

Mr. Christophe Ramu, ITER (International) provided a complementary perspective in his presentation titled *ITER organization's Experience Ensuring the Trustworthiness of Individuals Accessing Sensitive Locations or Information*. He began by briefly summarising the ITER project and listing some of the multiple organisations and countries that comprise this international project. He then described the process in place for ensuring the trustworthiness of individuals with access to sensitive locations within the facility and to sensitive information. In addition, Mr Ramu described current risks and how they would evolve as the project progresses. He also described some of the challenges faced in verifying the identity and trustworthiness of a workforce made of multiple nationalities and some of the physical measures implemented to support the administrative procedures. Finally, Mr Ramu highlighted how important sanctions for non-compliance with trustworthiness and access control procedures are to an effective insider mitigation programme.

After this series of presentations, participants were asked to form small groups, reflect on what they had heard, and identify some important take-aways. Some main findings included the importance of:

- Developing a graded approach to vetting.
- Consolidating statistical data (total number of applications, number of applications under processing, average duration for processing an application, % of rejected applications, etc.).
- Developing a good relationship (confidence) with intelligence agencies and other law enforcement organisations. (Identify point of contact, explain what you expect and need from them, tell them what you can bring to them, etc.)
- Having timely access to criminal records databases.
- International cooperation between law enforcement agencies to ensure effective vetting of foreign citizens.
- Establishing oversight mechanisms to ensure fairness/confidence in the vetting process.
- Properly addressing significant evolutions in work practices, conditions or environments (change management).
- Working closely with psychologists.
- Assessing line managers (reverse appraisal).
- Interviewing people used as personnel references in the application forms.
- Better engagement with the HR Department and maintaining security as a business enabler, not as an impediment.
- Understanding the cost of vetting and implementing clear funding mechanisms.

SESSION 6 - BEHAVIOURAL OBSERVATION PROGRAMMES AND PROCESSES FOR REPORTING SERIOUS CONCERNS

In Session 6, participants reviewed the purpose and benefits of behavioural observation tools and techniques. Discussions also covered the usual barriers and challenges for implementing these tools and techniques at the facility level and explored best practices for reporting serious concerns. The session also explored the role and content of a whistleblowing programme.

Mr Jeff Stevens, Bruce Power (Canada) opened Session 6 with a presentation titled *Behavioural Observation Program Practices and Lessons Learned*. After introducing his organisation, Mr Stevens described the organisational structure of nuclear security at Bruce Power and the applicable

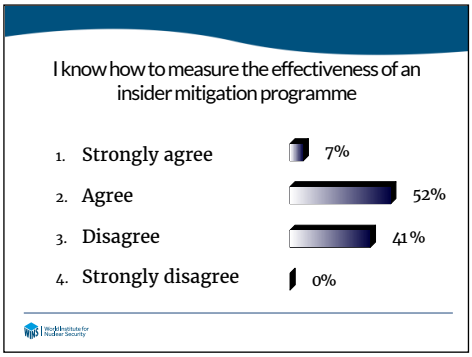
regulations. He explained the security awareness training opportunities available to staff and managers at Bruce Power and how certain elements of the insider mitigation programme are implemented. Mr Stevens then described Bruce Power's behavioural observation programme and shared some examples of reported and unreported incidents. Finally, he highlighted the importance of periodically testing and evaluating security arrangements and procedures.

In a presentation titled *Reporting Serious Concerns*, **Ms Beverley Oliver, Safe Call,** emphasised the importance of encouraging a speak-up culture and described some of the barriers that keep individuals from raising a concern. She also emphasised the need for management to make it clear to staff that they want to hear about any issues of concern. In addition, Ms Oliver encouraged participants to take ownership of this important matter and offered some best practices for doing so. She concluded her speech by stating that the culture of an organisation should encourage and enable open reporting, leading to learning and continuous improvement.

During the follow-up discussions, participants raised some important factors regarding the effective implementation of behavioural observation and reporting programmes. They emphasised the need for nuclear operators to educate the workforce about the value and benefit of such programmes, including creating a climate of honesty and transparency. They also emphasised the need for organisations to protect individual privacy when investigating issues and dealing with personal matters, as well as the importance of leading by example because staff will mirror the attitudes of their managers.

SESSION 7 – MEASURING THE EFFECTIVENESS OF INSIDER MITIGATION PROGRAMMES

The final session of Day 2 consisted of a brief discussion that allowed participants to share best practices for assessing the effectiveness of the arrangements implemented for mitigating the insider threat and to discuss possible performance indicators. The session opened with an E-vote to better understand how familiar participants were with methodologies for measuring the effectiveness of insider mitigation programmes. A large proportion of participants indicated a lack of knowledge and competency in this area. They also indicated that identifying key performance indicators and other relevant security metrics is challenging.



During follow-up discussions, participants discussed important issues related to assessing the effectiveness of the insider mitigation programme. Some of the discussion findings are reported below:

- **Testing and evaluation**. This is an essential element of the evaluation process. Small- and full-scale exercises should be conducted periodically. Key findings and lessons learned should be consolidated and shared. Awareness and culture can and should be measured (survey, audits, …). In addition to regulatory inspections, other assessment mechanisms, such as internal audits and peer reviews, are also effective approaches for assessing the performance of security arrangements and ensuring their continuous improvement.
- **Incident reporting and analysis**. Security related incidents should be documented and reported. They should be graded according to an incident scale and follow-up actions based on the severity level of the incident. Periodic reviews of past incidents (number, types, frequencies, common factors, etc.) should be conducted, and the main findings should be embedded into the continuous improvement process.

TUESDAY 18 DECEMBER 2018

The last day of the workshop was conducted at the Abu Dhabi IBM Innovation Centre, which enabled participants to explore insider cybersecurity issues. It also gave IBM the opportunity to showcase its security-related capabilities and provide insights on the use of Artificial Intelligence and analytics to strengthen security. The day was opened by Mr. Mitchel Free, IBM (USA) and Ms Mona Arishi, IBM (UAE)

SESSION 8 – ADDRESSING THE CYBER INSIDER THREAT

Session 8 focused on experiences in mitigating the cyber insider threat and provided an opportunity to review tools and techniques designed and implemented to counter this specific threat. Discussions covered both the nuclear experience and practices from other critical infrastructure.

Mr Anno Keizer, Urenco Netherlands opened the session with a presentation titled *Cyber Insider Threat*. After describing his organisation and its overall approach to risk management, he emphasised that the insider risk is real and complex. Threat can come from company employees, as well as from other individuals who access the site or Urenco IT systems. After a brief description of the possible types of insiders, Mr Keizer explained a few possible countermeasures. He concluded his presentation with some advice for enhancing a security programme against the cyber insider threat.

Mr Sultan Al Owais, Dubai Prime Minister Office (UAE) then delivered a session title *Cyber Insider Threat Mitigation in Industrial Environments*. After defining the problem, he explained the difference between cybersecurity and physical security. He also explained some high level design principles and highlighted areas that should receive priority. Mr Al Owais concluded with a warning against settling for short-term fixes and highlighted the need for long-term, structured efforts.

Follow-up discussions reiterated the risk related to the supply chain and the importance of strong control mechanisms. Participants also emphasised that awareness and training sessions for staff are a prerequisite for effective cybersecurity. Finally, participants agreed that people with a high level of knowledge, access and authority (such as system administrators) should receive particular attention and that various procedural (e.g. two-person rule) and technical (e.g. IT systems monitoring and analysis) measures should be implemented to reduce the risk.

SESSION 9 – IBM PRESENTATIONS AND DEMONSTRATIONS

Mr Ondrej Székely, IBM (Czech Republic) and Mr Michael Kehoe, IBM (Ireland) opened the IBM session with presentations on:

- IBM video analytics & introduction to artificial intelligence
- Artificial Intelligence use cases and video analytics demonstrations
- IBM security to help investigate insider threats

Participants where then split into sub-groups that rotated through a set of interactive sessions and live demonstrations of IBM's cybersecurity offering and of the SPEED helping IBM Client Base.

Closing Remarks and Workshop Evaluation

In his concluding remarks, Mr Legoux thanked participants for their active contributions during the workshop, which made the event a success. He encouraged them to continue discussing their experiences with each other in regard to protecting materials and facilities against the insider threat and to ensure that lessons learned are shared for the benefit of the entire community. Mr Legoux also committed WINS to building on this success and to continue offering opportunities for exchange and professional development to stakeholders involved in nuclear security.

During the plenary evaluation session, participants expressed a high level of satisfaction with the workshop. Many indicated that it had been an excellent learning experience and that they would recommend it to others. They also said they especially valued the amount of information shared, the diversity of the audience, and the varied perspectives.