Distinguished Delegates,
Ladies and Gentlemen, good morning.

It is an honor to address the Second CBRN International Congress as a Keynote Speaker. On behalf of the International Atomic Energy Agency (IAEA), I would like to thank the hosts, the Turkish Ministry of Interior Disaster and Emergency Management Presidency, for bringing together scientists, engineers, policy makers and legal experts committed to securing the world against Chemical, Biological, Radiological and Nuclear threats.

Whether we work in CBRN fields - we share an appreciation of the benefits of science and technology. Conversely, this Congress also share an appreciation of the dangers that can result when it falls in the wrong hands.

As we just heard in the preceding address, there will "be another threat along in a minute". I want to share the approach used by the IAEA to deal with evolving and emerging threats and technologies. I will discuss a few examples of novel approaches against current and emerging threats, and describe how through application of basic security principles, we may "best" address nuclear security threats. Finally, I will touch upon our approach for "sustaining" effective nuclear security strategies.

My first example is the un-manned aerial vehicle or UAV or more commonly known as a "drone". It may be regarded as a toy, a useful tool or even a threat.

Now, I want you to look at it from a peaceful use perspective. Think about commercial and medical applications. A drone could deliver medicines or food to people in distress during a natural disaster when roads are blocked or wide scale flooding occurs. Some of the bigger on-line shops are exploring how to use drones to deliver some of the millions of packages a day that are bought on-line.

In agricultural applications, drones are used by farmers to monitor crops and animal herds. They can be used to more efficiently and accurately apply pesticides and fertilizers to crops– reducing costs and reducing adverse environmental impacts.

In law enforcement applications, drones equipped with cameras can give police authorities a greatly expanded ability to monitor crowds and vehicles. The cameras can also feed facial recognition software and identify known individuals presenting possible threats. Drones equipped with radiation detectors can be used to search for a lost or stolen radiation source.

These are just a few of the peaceful applications of a technology that is evolving and advancing quickly. Now, I want you to think about drone technology from a malicious perspective. I spoke about delivery of medicines. Already, criminal are using drones to smuggle drugs and other contraband across borders – attempting to avoid the detection and interdiction systems and measures that are in place to counter traditional smuggling. Could drones then be used to smuggle nuclear materials across a border?

I spoke about farmers using drones to efficiently and effectively apply pesticides and fertilizers to crops. Could a terrorist group use a similar delivery system for a chemical or biological attack? What about using drones to deliver explosives in an attack on a chemical or a nuclear facility. As you likely know, there already was a recent drone attack against an oil refinery.

I spoke of law enforcement using drones to monitor crowds and detect threats. Could malicious actors use drones to monitor the presence and response of security and first responder forces in an attempt to avoid them? From a security perspective, we now have to consider the malicious uses of drones but also ways to detect and counter the drone threat.

I chose the drone example to show how quickly technology and threats evolve. Just a few years ago, the use of drones was much less limited from both peaceful and malicious perspectives.

If we want to be successful in meeting our CBRN security objectives, the security systems and measures we design and implement for addressing CBRN threats must be able to adapt and evolve as well. The processes we use for designing, implementing, and sustaining those systems and measures must account for the dynamic nature of threats and advances in technologies. I would argue that to be successful in this objective, science and technology must play a critical role in these processes and in the development of novel approaches.

The IAEA is the world's center for cooperation in the peaceful use of nuclear science and technology. In the current IAEA's Nuclear Security Plan 2018-2021, Member States underlined the importance of keeping pace with evolving challenges and threats to nuclear security using scientific and technological innovations and have affirmed the important role of science, technology, and engineering in understanding and addressing such challenges and threats.

It may seem an insurmountable challenge to address the myriad CBRN threats of today, but I believe it is possible through an integrated and coordinated approach using application of basic security principles with innovative use of science and technology, and with also a comprehensive legal-regulatory and resource framework.

When people think of nuclear security, the first thing that often comes to mind is a scene from a movie or television series: terrorists stealing nuclear material from heavily guarded nuclear facilities, sabotaging a nuclear power plant with a cyber-attack or attempting to detonate a dirty bomb. Storylines like these are popular, likely because they capture the imagination and reflect one of our worst fears.

But is nuclear security, or more broadly CBRN security, just guards, guns, and gates? I am convinced that guards, guns, gates AND GEEKS, provide better protection of nuclear and radioactive material and associated facilities; and prevent these scenarios from occurring in the real life. Science and technology are essential for robust nuclear security and provide many opportunities for scientists and engineers, the "geeks", to contribute to global security.

The IAEA refers to nuclear security as "the prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities." These three elements of nuclear security - prevention, detection and response, form an approach we all share- whether we are ensuring security of biological and chemical agents, or nuclear and other radioactive material.

Prevention: First, our security strategies must try to prevent an adversary from obtaining CBRN material; from carrying out an attack on a CBRN facility; or from using CBRN materials in an attack.

Imagine a city hospital with a highly radioactive Cobalt-60 source used for cancer therapy, or a chemical or biological lab with highly dangerous compounds or viruses. In many of these facilities, the doors to the room containing the dangerous materials will be reinforced with locks and sensors to prevent and indicate unauthorized access to the room. However, it is unlikely there will be an armed guard stationed there full-time. If an adversary breaks into the protected room, the alarms activate and security forces notified. For the physical protection system to be effective, it must be able to detect the break-in and delay the adversary long enough for the response force to arrive and apprehend the adversary.

The physical protection system must not only be "smart" enough to detect the attempt to access the dangerous material and delay even the best equipped adversary to allow sufficient time for response, but also sophisticated enough to prevent the ever-evolving adversaries from hacking the alarm notification system.

Recall my previous statement about guards, guns, and gates, how in the face of evolving threats and technologies do we assess the future effectiveness of our deployed security solutions and determine what changes in designs or security protocols we should make? Promising science and technology applications that the IAEA is using are game theory and 3-D visualization techniques to improve facility designs and to train security forces to better protect their facilities.

From 'inside' the computer simulated grounds of a hypothetical Nuclear Research Institute, trainees learn through realistic scenarios to work through the ins-and-outs of nuclear security threats and risks. Not only will users understand the physical protection systems and measures in place, but this new "computer game" also provides a novel approach for assessing the effectiveness of new sensors and processes to address evolving threats and changes in adversary tactics.

I have no doubt that advances in the gaming and simulation field, fueled by the ever increasing use of digital technologies, will continue to help us to develop more robust and ever-better systems for nuclear security.

However, as our IT and computing technologies increase, we must also keep in mind that not a day goes by that we do not read in the news of another cyber security attack on a computer-based system somewhere in the world. We must be wary in the nuclear security field of such attacks and look to protect our computer based systems from cyber-attack as well.

In this regard, the IAEA also has a robust cyber security program. We recently developed a two-week International training course (ITC) on protecting nuclear facilities from cyber-attack. The course offers participants a chance to test their skills on mock-ups of actual state-of-the-art digital systems common in today's nuclear facilities – facilities that use digital technologies to provide functions that support safe operations, security, material accountancy and control, and protection of sensitive information.

Now imagine that instead of securing a facility containing nuclear and radiological material, there is an illicit movement of nuclear or radioactive material out of regulatory control, or more broadly a CBRN material or weapon.

The priority here is **Detection**. At the IAEA, we look at detection as consisting of two approaches that should be integrated: detection by information and detection by instrument. Effective security detection strategies will involve extensive use of intelligence, commercial shipping documents, hospital reports of illnesses possibly caused by CBRN materials, etc. These important sources of information will assist in more effective deployment of limited resources and serve as early alerts to the presence of a threat. Additionally, instruments containing highly sensitive sensors deployed in airports, seaports, land crossings, and operated by our front line officers can be used to detect materials.

I want to focus for a moment on a critical issue of detection by instrument and a challenge across the CBRN spectrum. Our CBRN detection systems are often used in situations where one, the material that we want to detect is moving; or two, we have very short times to identify a threat using manpower that may not have in-depth technical knowledge; or three, the more sensitive our detectors, the

more likely our detectors will “false-alarm” on items innocently present in our physical background.

In nuclear security, we use the term “naturally occurring radioactive material” to broadly cover the radionuclides of natural origin that are abundant in our earth. A difficulty we face in nuclear detection is that the more sensitive we make our instruments to detect nuclear materials, the more likely we simply alarm on innocent products such as fertilizer, cement, or foods like soybeans and seaweed. Additionally, just variations in natural background radiation can cause an alarm as a detector is doing a mobile search.

I know that detectors for the other CBRN threat materials face similar problems.

To address issues with detectors and assessment of alarms, the IAEA has several Coordinated Research Projects (CRPs) underway. These projects use applied research to deliver sustainable security solutions and at the same time build capacity within the participating Member States. In the radiation detection area, we have three CRPs underway. These CRPs are providing tools to more efficiently, effectively and sustainably assess alarms; are developing better understanding of the capabilities and limitations of detection equipment and developing solutions and specifications to improve their performance; and are improving the Maintenance, Repair, and Calibration of Equipment to enhance the sustainability and effectiveness of detection equipment.

These CRPs bring experts, decision making authorities, and front line officers together to identify challenges and develop solutions. These CRPs also create the mechanism for continual strengthening of national nuclear security regimes based on the latest developments and innovative solutions; as well as provide invaluable collaboration opportunities for scientists and engineers.

The IAEA Division of Nuclear Security has 6 other CRPs underway involving institutes from over 50 countries. These applied research and development project are addressing security needs ranging from improvement of nuclear forensics techniques to innovative methods for identifying and countering insider threats.

One planned CRP that may be of particular interest to this Congress is a planned CRP on Facilitation of Safe and Secure Trade Using Nuclear Detection Technologies – with a focus on the detection of CBRNE and other contraband. The overall scope and objectives of this new CRP is currently under development, and research activities planned to start in mid-2020. Examples of planned activities under this CRP include: (1) improving technologies and processes using neutron interrogation to identify chemicals (explosives, drugs, chemicals) in shipping containers; (2) identifying methods for integration of passive and active systems to find shielded nuclear material; and (3) working with industry to better understand how to identify legitimate shipping practices and uses of material or equipment so that illicit activities can be more effectively detected.

These CRPs create the mechanism for continual strengthening of national nuclear security regimes based on the latest developments and innovative solutions; as well as provide invaluable collaboration opportunities for scientists and engineers.

While we rely on science and technology for efficacy of our physical protection systems to prevent an attack and to detect the illicit smuggling of nuclear material, we also rely on science and technology to respond to nuclear events, such as the interdiction of nuclear or radioactive material.

Questions such as: 1) what was the material's intended use; 2) what was the method of production, 3) and where was it produced and smuggled out of?- can be answered through nuclear forensic science. Physical characterization as well as chemical and isotopic measurements of the captured nuclear or radioactive material may identify the vulnerability at the origin facility. The results of these analyses also assist the law enforcement investigators with finding responsible parties and support the lawyers with prosecuting the adversaries within national legal frameworks.

At the beginning of my remarks, I stated I would discuss the IAEA approach for "sustaining" effective nuclear security strategies. National legal frameworks are part of a much larger policy and legal construct that is critical to sustaining effective and sustainable CBRN security.

International treaties, legally binding conventions, international standards and regulations, national legislation and laws must all support the development and implementation of effective CBRN security. Monitoring of facilities, controls on use and export of sensitive technologies and materials, training of experts and front line officers, awareness of the threat by government officials, and networks to support sustainability of solutions – all of these are part of an overall strategy.

While the responsibility for nuclear security within a State rests entirely with that State, IAEA remains concerned about the emerging threats to nuclear security, and therefore is committed to sustaining and strengthening nuclear security of all nuclear and other radioactive material and facilities in States, upon request. The Division of Nuclear Security and more broadly, the IAEA, uses a comprehensive approach to address all of the needed aspects of nuclear security. We support and provide oversight for treaties and conventions, assist in the development of laws and regulations, assist in upgrading security, assist in development and application of technologies, and assist in human resource development so that our Member States can develop and maintain the knowledge and capabilities needed to sustain nuclear security.

If the threat was always the same and did not adapt to our nuclear security measures, life would be easy. Unfortunately, threats adapt and the technologies and processes we use in nuclear security must be capable of adapting as well. We cannot afford to spend our efforts addressing the threats of the past, using technology and designs that are no longer effective or efficient. Resources in terms of manpower and financial costs are always tight. Whatever systems we design and implement, a nation or an organization must be able to afford to sustain.

The evolving nature of threats from CBRN devices, requires constant vigilance and awareness to provide safety and security in today's modern society. Awareness should include recognition of current and evolving threats, as well as understanding that novel approaches for the prevention of, detection of, and response to CBRN threats must use science and technology to provide adaptable, effective, and sustainable security solutions.

This Congress is a unique opportunity for all us to share our respective approaches to meeting the challenge of continuing to adapt- and anticipate- new and existing threats - and to leverage emerging science and technology toward greater security. I look forward to our discussions this week and to a successful Congress.

Thank you.